



NetIQ® Sentinel™

インストールと設定ガイド

2015年12月

保証と著作権

NetIQ の保証と著作権、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、および FIPS コンプライアンスの詳細については、<http://www.netiq.com/company/legal/> を参照してください。

Copyright © 2015 NetIQ Corporation. All Rights reserved.

NetIQ の商標については、<http://www.netiq.com/company/legal/> を参照してください。サードパーティの商標は、それぞれの所有者に属します。

目次

本書およびライブラリについて	9
NetIQ 社について	11
ページのパート I Sentinel について	13
1 Sentinel の概要	15
1.1 IT 環境のセキュリティ保護の課題	15
1.2 Sentinel が提供するソリューション	16
2 Sentinel の動作原理	19
2.1 イベントソース	21
2.2 Sentinel イベント	22
2.2.1 マッピングサービス	22
2.2.2 マップのストリーミング	23
2.2.3 エクスプロイト検出	23
2.3 コレクタマネージャ	23
2.3.1 コレクタ	23
2.3.2 コネクタ	24
2.4 エージェントマネージャ	24
2.5 NetFlow コレクタマネージャ	24
2.6 Sentinel データのルーティングとストレージ	25
2.7 関連	25
2.8 セキュリティインテリジェンス	26
2.9 インシデントの修復	26
2.10 iTrac ワークフロー	26
2.11 アクションとインテグレータ	26
2.12 検索	27
2.13 Reports (レポート)	27
2.14 ID トラッキング	27
2.15 イベント分析	27
ページのパート II Sentinel のインストール計画	29
3 実装チェックリスト	31
4 ライセンス情報について	33
4.1 Sentinel ライセンス	35
4.1.1 評価ライセンス	35
4.1.2 無償ライセンス	36
4.1.3 エンタープライズライセンス	36
5 システム要件を満たす	37
5.1 コネクタおよびコレクタのシステム要件	37
5.2 仮想環境	37

6	展開に関する考慮事項	39
6.1	分散展開の利点	39
6.1.1	追加のコレクタマネージャの利点	40
6.1.2	相関エンジンを追加することの利点	40
6.1.3	追加の NetFlow コレクタマネージャの利点	41
6.2	オールインワン展開	41
6.3	1 層分散展開	42
6.4	高可用性を備えた 1 層分散展開	43
6.5	2 層および 3 層分散展開	44
6.6	データストレージのパーティション計画	45
6.6.1	従来型インストールでのパーティションの使用	46
6.6.2	アプライアンスインストールでのパーティションの使用	46
6.6.3	パーティションレイアウトのベストプラクティス	46
6.6.4	Sentinel のディレクトリ構造	47
7	FIPS140-2 モードでの展開に関する考慮事項	49
7.1	Sentinel における FIPS 実装	49
7.1.1	RHEL NSS パッケージ	49
7.1.2	SLES NSS パッケージ	50
7.2	Sentinel の FIPS 実装コンポーネント	50
7.3	実装チェックリスト	51
7.4	導入シナリオ	52
7.4.1	シナリオ 1: 完全 FIPS 140-2 モードでのデータ収集	52
7.4.2	シナリオ 2: 部分 FIPS 140-2 モードでのデータ収集	53
8	使用するポート	55
8.1	Sentinel サーバのポート	56
8.1.1	ローカルポート	56
8.1.2	ネットワークポート	56
8.1.3	Sentinel サーバアプライアンス固有のポート	57
8.2	コレクタマネージャのポート	58
8.2.1	ネットワークポート	58
8.2.2	コレクタマネージャアプライアンス固有のポート	59
8.3	相関エンジンのポート	59
8.3.1	ネットワークポート	59
8.3.2	相関エンジンアプライアンス固有のポート	60
8.4	NetFlow コレクタマネージャのポート	60
9	インストールオプション	61
9.1	従来型インストール	61
9.2	アプライアンスインストール	62
	ページのパート III Sentinel のインストール	63
10	インストールの概要	65
11	インストールのチェックリスト	67
12	従来型インストール	69
12.1	インストールオプションについて	69

12.2	インタラクティブインストールの実行	70
12.2.1	Sentinel サーバの標準インストール	70
12.2.2	Sentinel サーバのカスタムインストール	71
12.2.3	コレクタマネージャと関連エンジンのインストール	73
12.3	サイレントインストールの実行	75
12.4	非 root ユーザとして Sentinel をインストール	76
13	アプライアンスインストール	79
13.1	Sentinel ISO アプライアンスのインストール	79
13.1.1	前提条件	79
13.1.2	Sentinel のインストール	80
13.1.3	コレクタマネージャと関連エンジンのインストール	81
13.2	Sentinel OVF アプライアンスのインストール	82
13.2.1	Sentinel のインストール	82
13.2.2	コレクタマネージャと関連エンジンのインストール	83
13.3	アプライアンスのインストール後の環境設定	84
13.3.1	WebYaST の環境設定	84
13.3.2	パーティションの作成	84
13.3.3	アップデートの登録	85
13.3.4	SMT でのアプライアンスの設定	86
13.3.5	VMware Tools のインストール (VMware ESX サーバにのみ適用)	87
13.4	WebYaST を使用したサーバの起動と停止	87
14	NetFlow コレクタマネージャのインストール	89
14.1	インストールのチェックリスト	89
14.2	NetFlow コレクタマネージャのインストール	89
15	コレクタとコネクタの追加インストール	93
15.1	コレクタのインストール	93
15.2	コネクタのインストール	93
16	インストールの検証	95
	ページのパート IV Sentinel の環境設定	97
17	時刻の設定	99
17.1	Sentinel における時刻について	99
17.2	Sentinel における時刻の設定	101
17.3	イベントの遅延時間限度の環境設定	101
17.4	タイムゾーンの処理	101
18	インストール後の環境設定の変更	103
19	付属プラグインの環境設定	105
19.1	プリインストールプラグインの表示	105
19.2	データコレクションの環境設定	105
19.3	ソリューションパックの環境設定	105
19.4	アクションとインテグレータの環境設定	106

20 既存の Sentinel インストール環境を FIPS 140-2 モードにする	107
20.1 Sentinel サーバを FIPS 140-2 モードで実行する	107
20.2 リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする	107
21 FIPS 140-2 モードでの Sentinel の運用	109
21.1 Advisor サービスを FIPS 140-2 モードで実行するように環境設定する	109
21.2 分散検索を FIPS 140-2 モードで実行するように環境設定する	109
21.3 LDAP 認証を FIPS 140-2 モードで実行するように環境設定する	111
21.4 リモートコレクタマネージャおよび関連エンジンのサーバ証明書の更新	111
21.5 Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する	112
21.5.1 エージェントマネージャコネクタ	112
21.5.2 データベース (JDBC) コネクタ	113
21.5.3 Sentinel Link コネクタ	113
21.5.4 Syslog コネクタ	114
21.5.5 Windows イベント (WMI) コネクタ	115
21.5.6 Sentinel Link インテグレータ	116
21.5.7 LDAP インテグレータ	117
21.5.8 SMTP インテグレータ	117
21.5.9 FIPS 140-2 モードの Sentinel で FIPS 非対応コネクタを使用する	117
21.6 証明書を FIPS キーストアデータベースにインポートする	118
21.7 Sentinel を非 FIPS モードに戻す	118
21.7.1 Sentinel サーバを非 FIPS モードに戻す	118
21.7.2 リモートコレクタマネージャまたはリモート関連エンジンを非 FIPS モードに戻す	119
ページのパート V Sentinel のアップグレード	121
22 実装チェックリスト	123
23 前提条件	125
23.1 カスタム環境設定情報の保存	125
23.2 Change Guardian の統合	125
23.3 Sentinel 7.1.1 より前のバージョンの場合の前提条件	125
24 従来の Sentinel インストールのアップグレード	127
24.1 Sentinel のアップグレード	127
24.2 非 root ユーザとしての Sentinel のアップグレード	128
24.3 コレクタマネージャまたは関連エンジンのアップグレード	130
25 Sentinel アプライアンスのアップグレード	133
25.1 zypper を使用したアプライアンスのアップグレード	133
25.2 WebYaST を使用したアプライアンスのアップグレード	135
25.3 SMT を使用したアプライアンスのアップグレード	136
26 アップグレード後の環境設定	139
26.1 JDBC DB2 ドライバの追加	139
26.2 Sentinel アプライアンスのデータフェデレーションプロパティの設定	139

27 Sentinel プラグインのアップグレード	141
ページのパート VI 高可用性のための Sentinel の展開	143
28 概念	145
28.1 外部システム	145
28.2 共有ストレージ	145
28.3 サービスの監視	146
28.4 フェンシング	146
29 システム要件	147
30 インストールと環境設定	149
30.1 初期セットアップ	150
30.2 共有ストレージのセットアップ	151
30.2.1 iSCSI Target の環境設定	152
30.2.2 iSCSI イニシエータの環境設定	153
30.3 Sentinel のインストール	154
30.3.1 最初のノードインストール	154
30.3.2 後続のノードインストール	156
30.4 クラスタインストール	157
30.5 クラスタ環境設定	158
30.6 リソースの環境設定	160
30.7 セカンダリストレージ設定	162
31 高可用性の Sentinel のアップグレード	165
31.1 前提条件	165
31.2 従来の Sentinel HA インストールのアップグレード	165
31.3 Sentinel HA アプライアンスインストールのアップグレード	167
31.3.1 Zypper を使用した Sentinel HA アプライアンスのアップグレード	167
31.3.2 WebYast を使用した Sentinel HA アプライアンスのアップグレード	169
32 バックアップと復元	171
32.1 バックアップ	171
32.2 回復	171
32.2.1 一時的な障害	171
32.2.2 ノードの破損	171
32.2.3 クラスタデータの設定	172
ページのパート VII 付録	173
A トラブルシューティング	175
A.1 ネットワーク接続が不正なためにインストールが失敗する	175
A.2 イメージを作成したコレクタマネージャまたは関連エンジンの UUID が作成されない	175
A.3 ログイン後に Internet Explorer で Web インタフェースがブランクになる	175
B アンインストール中	177
B.1 アンインストールのためのチェックリスト	177

B.2	Sentinel のアンインストール	177
B.2.1	Sentinel サーバのアンインストール	177
B.2.2	コレクタマネージャおよび相関エンジンのアンインストール	178
B.2.3	NetFlow コレクタマネージャのアンインストール	178
B.3	アンインストール後の作業	179

本書およびライブラリについて

本『インストールと設定ガイド』では、NetIQ Sentinel の概要を示し、Sentinel をインストールおよび設定する方法について説明します。

本書の読者

このガイドは、Sentinel 管理者およびコンサルタントを対象としています。

ライブラリに含まれているその他の情報

ライブラリには次の情報リソースが含まれています。

Administration Guide

Sentinel の展開を管理するために必要な管理情報および管理作業を説明します。

User Guide

Sentinel に関する概念情報を提供します。また、このマニュアルでは、ユーザインタフェースの概要を説明し、さまざまなタスクを手順を追って説明しています。

NetIQ 社について

当社はグローバルなエンタープライズソフトウェア企業であり、お客様の環境において絶えず挑戦となる変化、複雑さ、リスクという3つの要素に焦点を当て、それらをお客様が制御するためにどのようにサポートできるかを常に検討しています。

当社の観点

変化に適応すること、複雑さとリスクを管理することは普遍の課題

実際、直面するあらゆる課題の中で、これらは、物理環境、仮想環境、およびクラウドコンピューティング環境の安全な評価、監視、および管理を行うために必要な制御を脅かす最大の要因かもしれません。

重要なビジネスサービスの改善と高速化を可能にする

当社は、IT 組織に可能な限りの制御能力を付与することが、よりタイムリーでコスト効率の高いサービス提供を実現する唯一の方法だと信じています。組織が継続的な変化を遂げ、組織を管理するために必要なテクノロジーが実質的に複雑さを増していくにつれ、変化と複雑さという圧力はこれからも増え続けていくことでしょう。

当社の理念

単なるソフトウェアではなく、インテリジェントなソリューションを販売する

確かな制御手段を提供するために、まずお客様の IT 組織が日々従事している現実のシナリオを把握することに努めます。そのようにしてのみ、実証済みで測定可能な結果を成功裏に生み出す、現実的でインテリジェントな IT ソリューションを開発することができます。これは単にソフトウェアを販売するよりもはるかにやりがいのあることです。

当社の情熱はお客様の成功を推し進めること

お客様が成功するためにわたしたちには何ができるかということが、わたしたちのビジネスの核心にあります。製品の着想から展開まで、当社は次のことを念頭に置いています。お客様は既存資産とシームレスに連動して動作する IT ソリューションを必要としており、展開後も継続的なサポートとトレーニングを必要とし、変化を遂げるときにも共に働きやすいパートナーを必要としています。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

- ◆ ID およびアクセスのガバナンス
- ◆ アクセス管理
- ◆ セキュリティ管理
- ◆ システムおよびアプリケーション管理

- ◆ ワークロード管理
- ◆ サービス管理

セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通：	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ：	1-888-323-6768
電子メール：	info@netiq.com
Web サイト：	www.netiq.com

テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通：	www.netiq.com/support/contactinfo.asp
北米および南米：	1-713-418-5555
ヨーロッパ、中東、アフリカ：	+353 (0) 91-782 677
電子メール：	support@netiq.com
Web サイト：	www.netiq.com/support

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。改善のためのご提案は、www.netiq.com/documentationに掲載されている本マニュアルの HTML 版で、各ページの下にある [コメントを追加] をクリックしてください。Documentation-Feedback@netiq.com 宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQ のオンラインコミュニティである Qmunity は、他のユーザや NetIQ のエキスパートとやり取りできるコラボレーションネットワークです。より迅速な情報、有益なリソースへの役立つリンク、NetIQ エキスパートとのやり取りを提供する Qmunity は、頼みにしている IT 投資が持つ可能性を余すことなく実現するために必要な知識の習得に役立ちます。詳細については、<http://community.netiq.com> を参照してください。

Sentinel について

このセクションでは、Sentinel の概要と Sentinel が提供するイベント管理ソリューションについて詳しく説明します。

- ◆ [15 ページの第 1 章「Sentinel の概要」](#)
- ◆ [19 ページの第 2 章「Sentinel の動作原理」](#)

1 Sentinel の概要

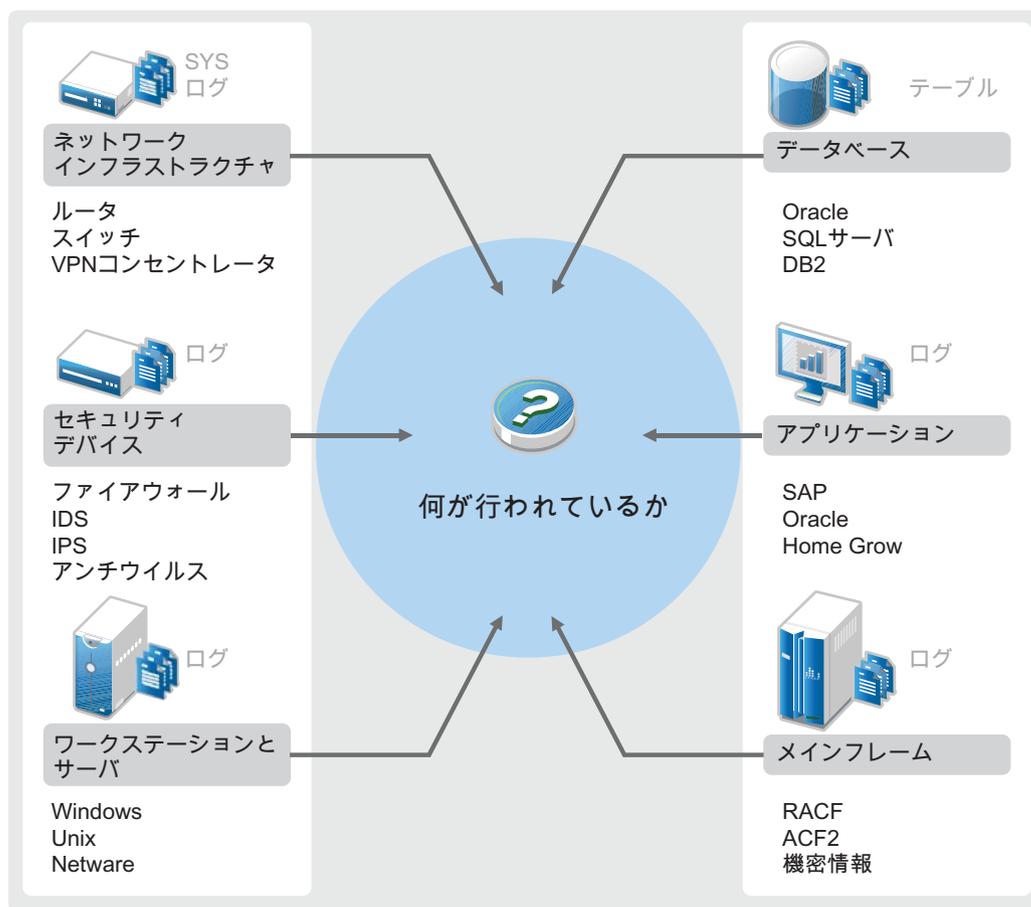
Sentinel は、セキュリティ情報およびイベント管理 (SIEM) ソリューションであると同時に、コンプライアンスモニタリングソリューションでもあります。Sentinel は、最も複雑な IT 環境を自動的にモニタリングし、IT 環境を保護するのに必要なセキュリティを提供します。

- ◆ 15 ページのセクション 1.1 「IT 環境のセキュリティ保護の課題」
- ◆ 16 ページのセクション 1.2 「Sentinel が提供するソリューション」

1.1 IT 環境のセキュリティ保護の課題

IT 環境のセキュリティ保護は、その環境が複雑であるため容易ではありません。一般に、IT 環境には多数のアプリケーション、データベース、メインフレーム、ワークステーションおよびサーバが存在し、それらすべてのエンティティがイベントのログを生成します。さらに、IT 環境にはセキュリティデバイスやネットワークインフラストラクチャデバイスもあり、それらのデバイスもイベントのログを生成する場合があります。

図 1-1 環境で発生していること



次の要因が、困難を生み出します。

- ◆ IT 環境にデバイスがたくさんある
- ◆ ログの形式が異なる
- ◆ さまざまな場所にログが保存される
- ◆ ログファイルに大量の情報が取り込まれる
- ◆ ログファイルを手動で分析しないとイベントのトリガを判断できない

ログファイルの情報を活用するには、次の作業を実行できる必要があります。

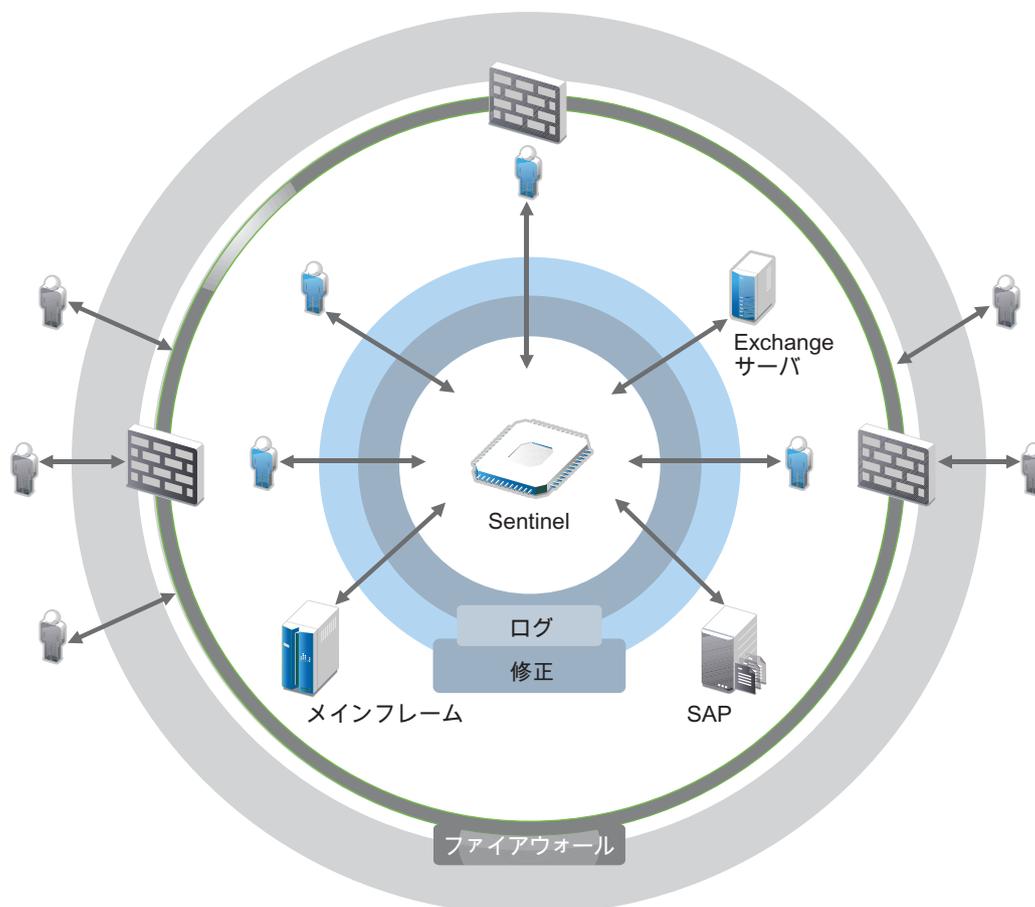
- ◆ データを収集する
- ◆ データを集約する
- ◆ 異種のデータを標準化してイベントにし、簡単に比較できるようにする
- ◆ イベントを標準規制に対応付けする
- ◆ データを分析する
- ◆ 複数のシステム間のイベントを比較し、セキュリティの問題があるかどうかを判断する
- ◆ データが基準から外れたときには通知を送信する
- ◆ ビジネスポリシーに従って通知に対する行動をとる
- ◆ コンプライアンスの証明のためにレポートを生成する

IT 環境のセキュリティ保護に関する課題について理解したら、ユーザエクスペリエンスを損なうことなく、ユーザのために企業のセキュリティを確保する方法と、ユーザから企業のセキュリティを保護する方法について判断することが必要になります。Sentinel がソリューションを提供します。

1.2 Sentinel が提供するソリューション

Sentinel は企業のセキュリティの中枢神経系として動作します。アプリケーション、データベース、サーバ、ストレージ、セキュリティデバイスなどのインフラストラクチャ全体からデータを収集します。データを分析して関連させ、データに自動または手動で対処できるようにします。

図 1-2 Sentinel が提供するソリューション



Sentinel では、IT 環境内にどの時点で発生した事態についても把握することができ、リソースに対して行われたアクションと、そのアクションを行った人物を結び付けることができます。これにより、ユーザの行動を特定し、アクティビティを能率的に監視して、悪意のあるアクティビティを防止することができます。

Sentinel では、次のようにして、これを実現しています。

- ◆ 複数のセキュリティ標準に及ぶ IT 制御に対応する単一のソリューションを提供する
- ◆ IT 環境内で発生するべき事象と実際に発生した事象の間にあるギャップを処理する
- ◆ セキュリティ標準への準拠を支援する
- ◆ すぐに使えるコンプライアンスモニタリングおよびレポーティングプログラムを提供する

Sentinel では、ログコレクション、分析、およびレポーティングプロセスを自動化することで、IT 制御により効果的に脅威の検出と監査要件に対応します。Sentinel は、セキュリティイベント、コンプライアンスイベント、および IT コントロールの自動モニタリングを提供します。これにより、セキュリティ違反または準拠違反のイベントが発生している場合に、すぐに対処できます。さらに、Sentinel を使用すると、自社環境についてのサマリ情報を収集することもできます。この情報は、主要な利害関係者と共有できます。

2 Sentinel の動作原理

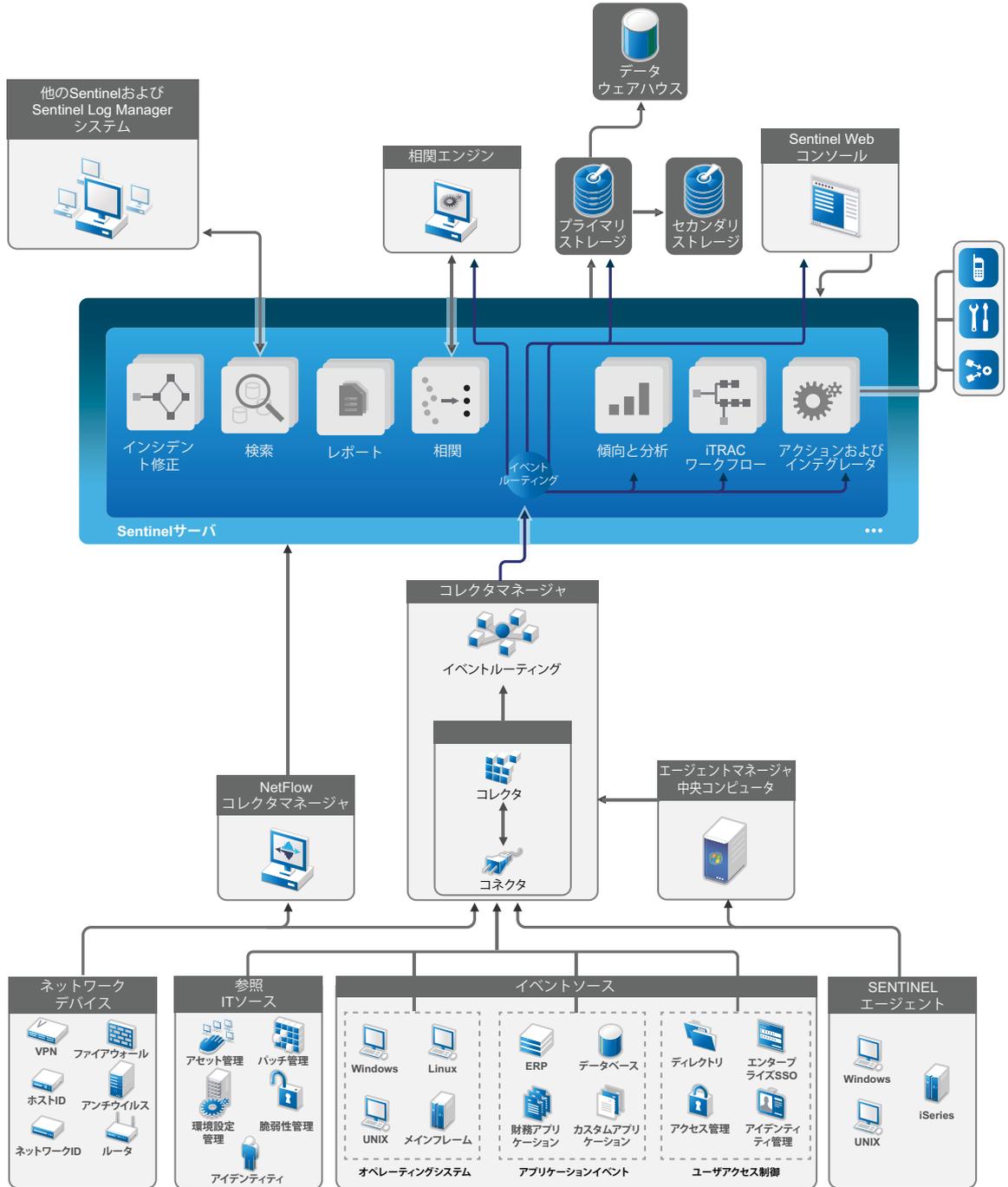
Sentinel は、IT 環境全体のセキュリティ情報とイベントを継続的に管理することで、完全なモニタリングソリューションを提供します。

Sentinel は次の処理を行います。

- ◆ IT 環境内のさまざまなソースからログ、イベント、およびセキュリティの情報を収集します。
- ◆ 収集したログ、イベント、およびセキュリティの情報を標準 Sentinel フォーマットに正規化します。
- ◆ 柔軟でカスタマイズ可能なデータ保持ポリシーを使用して、ファイルベースのデータストアにイベントを格納します。
- ◆ ネットワークフローデータを収集すると、ネットワークの動作を詳しく監視するのに役立ちます。
- ◆ Sentinel Log Manager を含む複数の Sentinel システムを階層的にリンクする機能を提供します。
- ◆ ローカルの Sentinel サーバ上のイベントに加えて、世界中に分散している Sentinel サーバ上のイベントも検索できる機能を提供します。
- ◆ 統計分析を実行してベースラインを定義し、そのベースラインと発生中の事象を比較して、未知の問題が発生していないかどうかを判断します。
- ◆ 特定の期間の類似または比較可能なイベントのセットを相関させて、パターンを特定します。
- ◆ 対応管理および追跡を効率的に行うため、イベントをインシデントにまとめます。
- ◆ リアルタイムおよび履歴イベントに基づいたレポートを提供します。

次の図は、Sentinel がどのように動作するのかを示しています。

図2-1 Sentinel のアーキテクチャ



以下のセクションでは、Sentinel コンポーネントについて詳しく説明します。

- ◆ 21 ページのセクション 2.1 「イベントソース」
- ◆ 22 ページのセクション 2.2 「Sentinel イベント」
- ◆ 23 ページのセクション 2.3 「コレクタマネージャ」
- ◆ 24 ページのセクション 2.4 「エージェントマネージャ」
- ◆ 24 ページのセクション 2.5 「NetFlow コレクタマネージャ」
- ◆ 25 ページのセクション 2.6 「Sentinel データのルーティングとストレージ」
- ◆ 25 ページのセクション 2.7 「相関」
- ◆ 26 ページのセクション 2.8 「セキュリティインテリジェンス」
- ◆ 26 ページのセクション 2.9 「インシデントの修復」
- ◆ 26 ページのセクション 2.10 「iTrac ワークフロー」
- ◆ 26 ページのセクション 2.11 「アクションとインテグレータ」
- ◆ 27 ページのセクション 2.12 「検索」
- ◆ 27 ページのセクション 2.13 「Reports (レポート)」
- ◆ 27 ページのセクション 2.14 「ID トラッキング」
- ◆ 27 ページのセクション 2.15 「イベント分析」

2.1 イベントソース

Sentinel は、IT 環境内のさまざまなソースからセキュリティ情報とイベントを収集します。このようなソースはイベントソースと呼ばれます。一般に、次のものがネットワーク上のイベントソースになります。

セキュリティの境界：環境にセキュリティ境界を作成するために使用される、ハードウェアとソフトウェアが組み込まれているセキュリティデバイス。ファイアウォール、侵入検知システム (IDS)、VPN (仮想プライベートネットワーク) などがあります。

オペレーティングシステム：ネットワーク内で実行されている各種オペレーティングシステム。

参照用 IT ソース：アセット、パッチ、環境設定、および脆弱性を保守および追跡するのに使用するソフトウェア。

アプリケーション：ネットワーク内にインストールされている各種アプリケーション。

ユーザアクセス制御：ユーザによる会社のリソースへのアクセスを許可するアプリケーションまたはデバイス。

イベントソースからイベントを収集する方法の詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Collecting and Routing Event Data](#)」を参照してください。

2.2 Sentinel イベント

Sentinel は、デバイスから情報を受信し、この情報をイベントと呼ばれる構造に正規化し、そのイベントを分類してから処理用に送信します。Sentinel は、カテゴリ情報 (taxonomy) をイベントに追加します。これにより、異なる方法でイベントをレポートするシステム全体でイベントを容易に比較できます。イベントは、リアルタイム表示、関連エンジン、ダッシュボード、およびバックエンドサーバによって処理されます。

1つのイベントは、200 を超えるフィールドで構成されます。イベントフィールドの種類と目的はさまざまです。重大度、深刻性、宛先 IP アドレス、宛先ポートなど、定義済みのフィールドがいくつかあります。

設定可能なフィールドのセットが2つあります。

- ◆ 予約済みフィールド：将来の機能拡張を可能にするために、Sentinel 内部で使用します。
- ◆ カスタムフィールド：カスタマイズのために、ユーザが使用します。

フィールドのソースは、外部または参照のどちらかになります。

- ◆ 外部フィールドの値は、デバイスまたは対応するコレクタにより明示的に設定されます。たとえば、イベントの宛先 IP アドレスとして指定されているアセットを含む建物の建物コードになるようフィールドを定義できます。
- ◆ 参照フィールドの値は、マッピングサービスを使用して1つ以上の他のフィールドに応じて計算されます。たとえば、イベントから得られる宛先 IP アドレスを使用して定義したマップを使用するマッピングサービスでフィールドを計算することができます。
- ◆ [22 ページのセクション 2.2.1 「マッピングサービス」](#)
- ◆ [23 ページのセクション 2.2.2 「マップのストリーミング」](#)
- ◆ [23 ページのセクション 2.2.3 「エクスプロイト検出」](#)

2.2.1 マッピングサービス

マッピングサービスにより、ビジネス関連のデータがシステム全体に伝播されます。このデータは、参照情報によってイベントを補足できます。

ソースデバイスからの着信イベントにホストや識別情報などの情報を追加するマップを使用することで、イベントデータを補足できます。Sentinel は、高度な相関とレポートに、この追加情報を使用できます。Sentinel は、複数の組み込みマップに加えて、カスタマイズされたユーザ定義のマップもサポートします。

Sentinel で定義されるマップは2つの方法で格納されます。

- ◆ 組み込みマップは、データベースに格納され、内部で更新されて、自動的にマッピングサービスにエクスポートされます。
- ◆ カスタムマップは、CSV ファイルとして格納され、ファイルシステム上または [マップデータの環境設定] ユーザインタフェースを使用して更新され、マッピングサービスによってロードされます。

いずれの場合も、CSV ファイルは中核となる Sentinel サーバに保存されますが、マップへの変更は、各コレクタマネージャに分散され、ローカルに適用されます。この分散処理で、マッピング動作によるメインサーバのオーバーロードを防止できます。

2.2.2 マップのストリーミング

マップサービスにはダイナミック更新モデルが採用されており、ある場所から別の場所にマップをストリーミングして、ダイナミックメモリ内に大きなスタティックマップが蓄積されないようにしています。これは、システムの一時的な負荷によって低下せず、安定して予測可能な素早いデータ移動を必要とする、Sentinel のようなミッションクリティカルなリアルタイムシステムにとって重要なことです。

2.2.3 エクスプロイト検出

Sentinel は、イベントデータ署名と脆弱性スキャナデータを相互参照する機能を提供します。脆弱なシステムに対してエクスプロイトが試行されると、即座に Sentinel は、自動的にユーザへ通知を送信します。Sentinel は、次の機能を使用して、これを実現しています。

- ◆ アドバイザのフィード
- ◆ 侵入検出
- ◆ 脆弱性スキャン
- ◆ ファイアウォール

Advisor フィードには、脆弱性と脅威、さらにイベント署名と脆弱性プラグインの正規化に関する情報が含まれます。Advisor は、イベントデータ署名と脆弱性スキャナデータとの相互参照を提供します。Advisor フィードの詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Detecting Vulnerabilities and Exploits](#)」を参照してください。

2.3 コレクタマネージャ

コレクタマネージャは、データ収集を管理し、システムステータスメッセージを監視し、イベントフィルタリングを実行します。コレクタマネージャの主要な機能は次のとおりです。

- ◆ コネクタの使用によるデータの収集。
- ◆ コレクタの使用によるデータの解析と正規化。

2.3.1 コレクタ

コレクタは、コネクタから情報を収集して、その情報を正規化します。コレクタは、次の機能を実行します。

- ◆ 生データをコネクタから受信する。
- ◆ データの解析と正規化を実行する。
 - ◆ イベントソース固有のデータを Sentinel 固有のデータに変換する。
 - ◆ イベントに含まれる情報を Sentinel が読み込めるフォーマットに変更してイベントを補強する。
 - ◆ イベントにイベントソース固有のフィルタリングを行う。
- ◆ マッピングサービスによってイベントにビジネスとの関連性を追加する：
 - ◆ イベントを識別情報にマッピングする。
 - ◆ イベントをアセットにマッピングする。

- ◆ イベントをルーティングする
- ◆ 正規化、解析、および形式設定を行ったデータをコレクタマネージャに渡す。
- ◆ ヘルスメッセージを Sentinel サーバに送信する

コレクタの詳細については、[Sentinel プラグイン Web サイト](#)を参照してください。

2.3.2 コネクタ

コネクタにより、イベントソースから Sentinel システムへの接続が提供されます。

コネクタが提供する機能は、次のとおりです。

- ◆ イベントソースからコレクタへの生イベントデータの転送。
- ◆ 接続固有のフィルタリング。
- ◆ 接続エラー処理。

2.4 エージェントマネージャ

エージェントマネージャにより、ホストベースのデータ収集が可能になります。これは、ユーザが次のタスクを実行できるようにすることで、エージェントを使用しないデータ収集を補完するものです。

- ◆ ネットワーク経由では利用できないログへのアクセス。
- ◆ 厳重に管理されたネットワーク環境で運用する。
- ◆ 基幹サーバの攻撃露呈部分を制限することにより、セキュリティ体制を向上する。
- ◆ ネットワーク中断時も信頼性の高いデータ収集を行う。

エージェントマネージャを使用すると、エージェントの展開とエージェント設定の管理ができるようになります。また、エージェントマネージャは、Sentinel に流れ込むイベントの収集ポイントとしても機能します。エージェントマネージャの詳細については、[エージェントマネージャの資料](#)を参照してください。

2.5 NetFlow コレクタマネージャ

NetFlow コレクタマネージャはルータ、スイッチ、ファイアウォールなどのネットワークデバイスからネットワークフローデータ (NetFlow や IPFIX など) を収集します。ネットワークフローデータにより、すべてのホスト間のネットワーク接続に関する基本情報が示されます。この情報には、送信したパケット数やバイト数が含まれています。これは、個別のホストまたはネットワーク全体の振る舞いを視覚化する際に役立ちます。

NetFlow コレクタマネージャは、次の機能を実行します。

- ◆ サポートされているネットワークデバイスからのバイト、フロー、およびパケット単位でのネットワークフローデータの収集。
- ◆ 収集されたデータの集約および Sentinel サーバへの送信。これにより、ご使用の環境でのネットワークの動作の視覚化および分析が行われます。

ネットワークフローデータの視覚化および分析について詳しくは、『[NetIQ Sentinel User Guide](#)』の「[Visualizing and Analyzing Network Flow Data](#)」を参照してください。

2.6 Sentinel データのルーティングとストレージ

Sentinel は、収集したデータをルーティング、保存、および抽出するためのさまざまなオプションを備えています。デフォルトでは、Sentinel は解析済みイベントデータと生データをコレクタマネージャから受信します。Sentinel は、セキュアなエビデンスチェーンを提供するために生データを保護されたパーティションに保存します。解析済みイベントデータはユーザ定義のルールに従ってルーティングされます。解析済みイベントデータはフィルタ処理することで、ストレージやリアルタイム分析に送信することも、外部システムにルーティングすることもできます。さらに、Sentinel はストレージに送信されるすべてのイベントデータをユーザ定義の保存ポリシーと照合して、どのパーティションにデータを配置するかを決定します。また、グルーミングポリシーを定義して、イベントデータの保持と最終的な削除の際に、このポリシーを使用します。

Sentinel のデータストレージは、3 層構造になっています。

オンラインストレージ	プライマリストレージ (以前のローカルストレージ)。	迅速な書き込みと高速な取得のために最適化されています。最後に収集されたイベントデータと最も頻りに検索されたイベントデータを保存します。
	セカンダリストレージ (以前のネットワークストレージ)。(オプション)	高速データ取得をサポートしながら、安価なストレージ上の領域使用量を削減するように最適化されています。Sentinel は自動的にデータパーティションをセカンダリストレージに移行します。
		注: セカンダリストレージの使用はオプションです。データ保持ポリシー、検索、およびレポートは、プライマリストレージとセカンダリストレージのどちらに存在するか、あるいは両方存在するかにかかわらず、イベントデータパーティションで実行されます。
オフラインストレージ	アーカイバルストレージ	パーティションが閉じられているときには、そのパーティションを任意のファイルストレージサービス (Amazon Glacier など) にバックアップできます。そのパーティションは、長期的なフォレンジック分析に使用するために、いつでも一時的に再インポートできます。

データ同期ポリシーを使用して、イベントデータとイベントデータ要約を外部データベースに抽出するように Sentinel を設定することもできます。詳細については、『[NetIQ Sentinel Administration Guide \(NetIQ Sentinel 7.0.1 管理ガイド\)](#)』の「[Configuring Data Synchronization \(データ同期の設定\)](#)」を参照してください。

2.7 関連

単一のイベントでは取るに足りないように思えても、別のイベントと組み合わせると潜在的な問題の警告になることがあります。Sentinel では、ユーザが作成して関連エンジンに展開したルールを使用して、このようなイベントを関連させ、適切な対策を講じて問題を緩和することができます。

関連関係により、受信するイベントストリームの分析を自動化し、特定のパターンを発見できるため、セキュリティイベント管理のインテリジェンスが高まります。関連関係により、重大な脅威や複雑な攻撃パターンを識別するルールを定義できることで、イベントに優先順位をつけるとともに、効果的なインシデント管理と対応が可能になります。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Correlating Event Data](#)」を参照してください。

関連ルールに従ってイベントを監視するには、関連ルールを関連エンジンに展開する必要があります。ルールの条件と一致するイベントが発生すると、関連エンジンはそのパターンを記述する関連イベントを生成します。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Correlation Engine](#)」を参照してください。

2.8 セキュリティインテリジェンス

Sentinel の関連機能により、アクティビティの既知のパターンを見つけられるようになります。このパターンは、セキュリティ、コンプライアンス、またはその他の理由を目的として分析できます。セキュリティインテリジェンス機能は、通常のアクティビティから外れていて、悪意の可能性があるが、既知のパターンとは一致しないアクティビティを検出します。

Sentinel のセキュリティインテリジェンス機能は、時系列データの統計分析を採用しており、自動化された統計エンジンまたは手動解釈用の統計データの視覚表示によって、分析者が異常を識別して分析できるようにします。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Analyzing Trends in Data](#)」を参照してください。

2.9 インシデントの修復

Sentinel は、自動インシデント応答管理システムを備えているため、インシデントやポリシー違反の追跡、エスカレート、対応についてのプロセスを文書化および形式化することができます。また、トラブルチケットシステムとの双方向の連携も可能になります。Sentinel により、インシデントに迅速に対応し、効率的に解決できるようになります。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Configuring Incidents](#)」を参照してください。

2.10 iTrac ワークフロー

iTRAC ワークフローは、企業のインシデント対応プロセスの自動化および追跡を行うための、シンプルで柔軟性のあるソリューションを提供します。iTRAC は Sentinel の内部インシデントシステムを活用し、関連ルールまたは手動識別による識別から始まり解決に至るまで、セキュリティやシステム上の問題を追跡できます。

ワークフローは、手動ステップと自動ステップを使用して構築できます。iTrac のワークフローでは、分岐、時間ベースのエスカレーション、およびローカル変数などの高度な機能がサポートされています。外部のスクリプトおよびプラグインとの統合により、サードパーティシステムとの柔軟なやり取りが可能になります。包括的なレポートングにより、管理者はインシデント応答プロセスを理解し、微調整することができます。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Configuring iTRAC Workflows](#)」を参照してください。

2.11 アクションとインテグレータ

アクションは、メールの送信など、何らかのタイプのアクションを手動または自動で実行します。アクションは、ルーティングルール、イベントやインシデント操作の手動実行、および関連ルールでトリガできます。Sentinel には、一連の事前定義アクションが提供されています。デフォルトのアクションを使用し必要に応じてそれらを再設定するか、新規のアクションを追加することができます。詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Configuring Actions](#)」を参照してください。

アクションを単独で実行することも、インテグレータプラグインで設定したインテグレータインスタンスを利用することもできます。インテグレータプラグインは、Sentinel 修正アクションの特長と機能性を拡充します。インテグレータによって、LDAP サーバ、SMTP サーバ、SOAP サーバなどの外部システムに接続してアクションを実行することができます。詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Configuring Integrators](#)」を参照してください。

2.12 検索

Sentinel は、イベントに対して検索を実行するオプションを提供しています。プライマリストレージまたはセカンダリストレージの場所にあるデータを検索できます。必要な環境設定により、Sentinel によって生成されたシステムイベントを検索して、イベントごとに生データを表示することもできます。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Performing a Search](#)」を参照してください。

複数の地理的場所に分散した Sentinel サーバを検索することもできます。詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Configuring Data Federation](#)」を参照してください。

2.13 Reports (レポート)

Sentinel では、収集したデータについてのレポートを実行できます。Sentinel には、さまざまな種類のカスタマイズ可能なレポートがパッケージとして含まれています。結果に表示するカラムを指定できる、構成可能なレポートもあります。

PDF フォーマットのレポートを実行することも、スケジュールすることも、電子メールで送信することもできます。また、任意のレポートを検索として実行し、検索条件を絞ったり結果に対してアクションを実行したりするなど、検索の場合と同じように結果を操作することができます。地理的に異なる場所に分散している Sentinel サーバ上でレポートを実行することもできます。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Reporting](#)」を参照してください。

2.14 ID トラッキング

Sentinel は、ID 管理システムに、各ユーザアカウントの ID とそれらの ID が実行するイベントを追跡するための統合フレームワークを提供します。また、連絡先情報、ユーザアカウント、最近の認証イベント、最近のアクセスイベント、パーミッション変更などのユーザ情報も提供します。特定のアクションを開始した人物やアクションの影響を受ける人物に関する情報を表示することで、Sentinel はインシデント対応時間を短縮し、振る舞いベースの分析を可能にします。詳細については、『[NetIQ Sentinel User Guide](#)』の「[Leveraging Identity Information](#)」を参照してください。

2.15 イベント分析

Sentinel には、重大なイベントデータの検索と分析を簡単にする強力なツールのセットが用意されています。Sentinel は、あらゆるタイプの分析で効率が最大になるようにシステムを最適化し、あるタイプの分析から別のタイプの分析へのシームレスで簡単な移行方法を提供しています。

Sentinel でのイベントの調査は、ほぼリアルタイムのアクティブビューで開始する場合があります。さらに高度なツールも使用できますが、アクティブビューはフィルタされたイベントストリームをサマリチャートと一緒に表示するため、イベントの傾向とイベントデータのシンプルで手早い分析や、特定のイベントの識別に使用できます。時間の経過と共に、相関からの出力など、特定のクラスのデータに合わせて調整したフィルタを構築できるようになります。アクティブビューは、運用とセキュリティに関する全般的な方針を示すダッシュボードとして使用できます。

さらに、インタラクティブ検索を使用して、詳細なイベントの分析を実行できます。これにより、特定のユーザや特定のシステムによるアクティビティなど、特定のクエリに関連するデータをすばやく簡単に検索して見つけることができます。イベントデータをクリックしたり、左側の絞り込みウィンドウを使用すると、簡単に目的のイベントに焦点を絞ることができます。

多数のイベントを分析する場合でも、Sentinel のレポート機能にはイベントのレイアウトに対するカスタムコントロールが用意されているため、大量のデータを表示できます。Sentinel では、検索インターフェイスで構築したインタラクティブ検索をレポートテンプレートに移動できるため、この移行が簡単になります。これにより、多数のイベントにより適したフォーマットで同じデータを表示するレポートをすぐに作成できます。

Sentinel には、これを目的としたレポートテンプレートが多数含まれています。レポートテンプレートには、2つのタイプがあります。

- ◆ 特定のタイプの情報 (認証データやユーザ作成など) の表示に合わせて微調整されたテンプレート。
- ◆ レポート上のグループと列を対話的にカスタマイズできる汎用テンプレート。

時間の経過と共に、共通して使用するフィルタとレポートを開発して、ワークフローをより簡単にできます。Sentinel では、この情報の保存と、組織内のユーザへの配布がサポートされています。詳細については、『[NetIQ Sentinel User Guide](#)』を参照してください。

Sentinel のインストール計画

次に示す各章では、Sentinel のインストール計画について順を追って説明しています。以降の章で特定されていない構成をインストールする場合や質問がある場合は、[NetIQ テクニカルサポート](#)までお問い合わせください。

- ◆ 31 ページの第 3 章「実装チェックリスト」
- ◆ 33 ページの第 4 章「ライセンス情報について」
- ◆ 37 ページの第 5 章「システム要件を満たす」
- ◆ 39 ページの第 6 章「展開に関する考慮事項」
- ◆ 49 ページの第 7 章「FIPS140-2 モードでの展開に関する考慮事項」
- ◆ 55 ページの第 8 章「使用するポート」
- ◆ 61 ページの第 9 章「インストールオプション」

3 実装チェックリスト

Sentinel の計画、インストール、および環境設定を実行する場合は、次に示すチェックリストを使用してください。

以前のバージョンの Sentinel からアップグレードする場合は、このチェックリストを使用しないでください。アップグレードの詳細については、[121 ページのパート V 「Sentinel のアップグレード」](#)を参照してください。

タスク	参照先
☐ Sentinel コンポーネントについて知るために、製品のアーキテクチャ情報を確認します。	13 ページのパート I 「Sentinel について」
☐ Sentinel のライセンス情報を確認して、Sentinel の評価ライセンスとエンタープライズライセンスの、どちらのライセンスを使用する必要があるかを判断します。	33 ページの第 4 章 「ライセンス情報について」
☐ ハードウェア構成を確認するために、使用している環境を評価します。Sentinel およびそのコンポーネントのインストール先となるコンピュータが指定された要件を満たしていることを確認します。	37 ページの第 5 章 「システム要件を満たす」
☐ コレクタマネージャと関連エンジンの 1 秒あたりのイベント数 (EPS) と、NetFlow コレクタマネージャの 1 秒あたりのレコード数 (RPS) に基づいて、使用する環境に適した展開の種類を決定します。 パフォーマンスおよび負荷分散を向上させるためにインストールする必要がある、コレクタマネージャ、関連エンジン、および NetFlow コレクタマネージャの数を決定します。	39 ページのセクション 6.1 「分散展開の利点」 .
☐ 最新の Sentinel リリースノートで、新機能と既知の問題を確認します。	Sentinel リリースノート
☐ Sentinel をインストールします。	63 ページのパート III 「Sentinel のインストール」
☐ Sentinel サーバで時刻を設定します。	99 ページの第 17 章 「時刻の設定」
☐ Sentinel をインストールすると、その Sentinel リリースの時点で利用可能な Sentinel プラグインがデフォルトでインストールされます。インストール直後のプラグインを、データ収集とレポート作成の用途に合わせて設定します。	105 ページの第 19 章 「付属プラグインの環境設定」 .

タスク	参照先
<ul style="list-style-type: none"> □ Sentinel には、すぐに使える相関ルールが付属しています。一部の相関ルールは、ルールの起動時に電子メールを送信するアクション ([Notify Security Admin] アクションなど) を実行するようデフォルトで設定されています。そのため、SMTP インテグレータと Send Email アクションを設定することで、Sentinel サーバのメールサーバ設定を構成する必要があります。 	<p>SMTP インテグレータと Send Email アクションの資料は、Sentinel Plug-ins Web サイトにあります。</p>
<ul style="list-style-type: none"> □ ご使用の環境で必要であれば、コレクタとコネクタを追加インストールします。 	<p>93 ページの第 15 章「コレクタとコネクタの追加インストール」。</p>
<ul style="list-style-type: none"> □ ご使用の環境で必要であれば、コレクタマネージャと相関エンジンを追加インストールします。 	<p>63 ページのパート III「Sentinel のインストール」</p>

4 ライセンス情報について

Sentinel には、お客様の多様なニーズに応えるための多彩な機能が含まれています。目的に適ったライセンスモデルを選択してください。

Sentinel プラットフォームでは、次の 2 つのライセンスモデルを提供しています。

- ◆ **Sentinel Enterprise:** フル機能のソリューションで、すべての主要なリアルタイムのビジュアル分析機能と、他の多くの機能を使用できます。Sentinel Enterprise は、リアルタイムの脅威の検出、アラート、修正など、SIEM のユースケースに重点を置いています。
- ◆ **Sentinel for Log Management:** データの収集、保存、検索、およびレポートなど、ログ管理用のソリューションです。

Sentinel for Log Management は、Sentinel Log Manager 1.2.2 の機能の大幅なアップグレードで、設計の大部分が変更されているものもあります。Sentinel for Log Management へのアップグレードを計画している場合は、[Sentinel FAQ ページ](#)を参照してください。

購入されたソリューションとアドオンに応じて、NetIQ は Sentinel の正当な機能を使用できるようにする、適切なライセンスキーとエンタイトルメントを提供します。ライセンスキーとエンタイトルメントにより、製品の機能とダウンロードへの基本的なアクセスが管理されますが、追加の条項については購入契約とエンドユーザ使用許諾契約を参照する必要があります。

次の表では、各ソリューションで使用できる具体的なサービスや機能について説明します。

表 4-1 Sentinel のサービスと機能

サービスと機能	Sentinel Enterprise	Sentinel for Log Management
主要な機能	対応	対応
<ul style="list-style-type: none"> ◆ 基本のイベントコレクション ◆ イベント以外のデータコレクション (アセット、脆弱性、ID) ◆ 解析と正規化 ◆ イベントデータの分類学的分類 ◆ インライン文脈マッピング ◆ Netflow のコレクションとストレージ ◆ リアルタイムでの NetFlow の可視化 ◆ イベントに基づいた NetFlow の可視化 ◆ イベントの検索 (ローカル) ◆ イベントのレポートिंग ◆ イベントのフィルタリング ◆ リアルタイムのイベントの可視化 ◆ イベントの保存 ◆ データ保持のポリシー ◆ イベントストアの否認防止 ◆ 連邦情報処理標準刊行物 140-2 (FIPS 140-2) イネーブルメント ◆ 手動で起動されたアクション ◆ 手動によるインシデントの作成と管理 ◆ インシデントのアクションとワークフロー ◆ iTRAC ワークフロー 		
Actions (アクション)	対応	対応
<ul style="list-style-type: none"> ◆ 相関を起動したアクション(相関が有効になっている場合のみ) ◆ ルーティングルールを起動したアクション(ルールが有効になっている場合のみ) ◆ 手動で起動されたアクション 		
ルーティングルール	対応	対応
<ul style="list-style-type: none"> ◆ イベントルーティング (外部) ◆ ルーティングルールによって起動されたアクション (アクションが有効になっている場合のみ) 		
Sentinel Link	対応	対応

サービスと機能	Sentinel Enterprise	Sentinel for Log Management
相関 <ul style="list-style-type: none"> リアルタイムのパターン相関 相関ルールによって起動されたアクション(アクションが有効になっている場合のみ) アラートトリアージ アラートダッシュボード 	対応	非対応
データ同期	対応	対応
アーカイブからのイベントデータの復元	対応	対応
データフェデレーション(分散検索)	対応	対応
エクスプロイト検出(Advisor)	対応	対応
セキュリティインテリジェンス <ul style="list-style-type: none"> アノマリールール リアルタイムの統計分析 	対応	非対応

4.1 Sentinel ライセンス

このセクションでは、Sentinel のライセンスの種類に関する情報を提供します。

- ◆ [35 ページのセクション 4.1.1 「評価ライセンス」](#)
- ◆ [36 ページのセクション 4.1.2 「無償ライセンス」](#)
- ◆ [36 ページのセクション 4.1.3 「エンタープライズライセンス」](#)

4.1.1 評価ライセンス

デフォルトの評価ライセンスでは、一定の評価期間中に Sentinel Enterprise のすべての機能を、ハードウェアの容量に応じて EPS 制限なしで使用できます。Sentinel Enterprise で使用できる機能については、[34 ページの表 4-1 「Sentinel のサービスと機能」](#)を参照してください。

システムの有効期限は、システム内で最も古いデータに基づきます。古いイベントをシステムに復元すると、Sentinel はそれに応じて有効期限を更新します。

評価ライセンスの期限が切れると、システムは基本の、無料ライセンスで実行されます。このライセンスで使用できる機能は一部のみに制限され、イベント数も 25 EPS に制限されます。

エンタープライズライセンスにアップグレードすると、Sentinel にすべての機能が戻ります。機能の中断を防ぐには、評価ライセンスが切れるまでにシステムをエンタープライズライセンスでアップグレードする必要があります。

4.1.2 無償ライセンス

無償ライセンスでは、一部の機能のみが使用でき、イベント数が 25EPS に制限されます。

無償ライセンスでは、イベントを収集したり保管したりできます。EPS 数が 25 を超えると、Sentinel は受信したイベントを保管しますが、それらのイベントの詳細は検索結果やレポートには表示されません。Sentinel は、これらのイベントに OverEPSLimit タグを付けます。

無償ライセンスには、リアルタイム機能はありません。ライセンスをエンタープライズライセンスにアップグレードすることで、すべての機能を戻すことができます。

注：NetIQ は、Sentinel の無償版のテクニカルサポートおよび製品アップデートは提供していません。

4.1.3 エンタープライズライセンス

Sentinel を購入すると、お客様向けポータルから、ライセンスキーを受け取ります。購入したライセンスに応じた機能、データ収集レート、およびイベントソースがライセンスキーで有効になります。ライセンスキーでは強制されない追加のライセンス条件が存在することがあるため、使用許諾契約は十分に確認してください。

ライセンスを変更する場合は、アカウントマネージャにお問い合わせください。

エンタープライズライセンスキーは、インストール時またはそれ以降いつでも追加できます。ライセンスキーを追加するには、『[NetIQ Sentinel Administration Guide](#)』の「[Adding a License Key](#)」を参照してください。

5 システム要件を満たす

Sentinel の実装は IT 環境のニーズに応じて異なるため、目的の環境に適った Sentinel のアーキテクチャを最終決定する前に、[NetIQ コンサルティングサービス](#)または [NetIQ Sentinel パートナー](#)にお問い合わせください。

推奨されるハードウェア、サポートされるオペレーティングシステム、アプライアンスのプラットフォーム、およびブラウザの詳細については、[NetIQ Sentinel 技術情報の Web サイト](#)を参照してください。

- ◆ [37 ページのセクション 5.1 「コネクタおよびコレクタのシステム要件」](#)
- ◆ [37 ページのセクション 5.2 「仮想環境」](#)

5.1 コネクタおよびコレクタのシステム要件

各コネクタおよびコレクタには、それぞれ独自のシステム要件およびサポートされるプラットフォームがあります。[Sentinel プラグイン Web サイト](#)で、コネクタとコレクタのマニュアルを参照してください。

5.2 仮想環境

Sentinel は、VMware ESX サーバでサポートされています。仮想環境を設定する場合、仮想マシンには複数の CPU が必要です。ESX 上の物理マシンや、その他の仮想環境におけるテストの結果と同等のパフォーマンス結果を達成するには、仮想環境が物理マシンで推奨される内容と同じメモリ、CPU、ディスク容量、および I/O を備える必要があります。

物理マシンの推奨事項の詳細については、[NetIQ Sentinel 技術情報の Web サイト](#)を参照してください。

6 展開に関する考慮事項

Sentinel は、必要な負荷に応じて拡張する、スケーラブルなアーキテクチャを備えています。この章では、Sentinel 展開のスケーリング時に考慮すべき重要な事項について簡単に説明します。NetIQ テクニカルサポートまたは NetIQ Partner Services の専門家が、目的の IT 環境に適した Sentinel システムの設計を支援します。

- ◆ 39 ページのセクション 6.1 「分散展開の利点」
- ◆ 41 ページのセクション 6.2 「オールインワン展開」
- ◆ 42 ページのセクション 6.3 「1 層分散展開」
- ◆ 43 ページのセクション 6.4 「高可用性を備えた 1 層分散展開」
- ◆ 44 ページのセクション 6.5 「2 層および 3 層分散展開」
- ◆ 45 ページのセクション 6.6 「データストレージのパーティション計画」

6.1 分散展開の利点

Sentinel サーバには、デフォルトで以下のコンポーネントが含まれます。

- ◆ **コレクタマネージャ**：コレクタマネージャは、Sentinel に柔軟なデータ収集ポイントを提供します。Sentinel インストーラは、インストール時にデフォルトでコレクタマネージャをインストールします。
- ◆ **相関エンジン**：相関エンジンは、リアルタイムイベントストリームからのイベントを処理して、イベントが何らかの相関ルールをトリガするべきかどうかを判別します。
- ◆ **NetFlow コレクタマネージャ**：NetFlow コレクタマネージャはルータ、スイッチ、ファイアウォールなどのネットワークデバイスからネットワークフローデータ (NetFlow や IPFIX など) を収集します。ネットワークフローデータは、伝送されるパケットやバイトなどの、ホストの間のすべてのネットワーク接続に関する基本的な情報を示しています。これは、個々のホストまたはネットワーク全体の動作を視覚化するのに役立ちます。

重要：運用環境では、分散展開をセットアップして、データ収集コンポーネントが別のコンピュータに分離することをお勧めします。これは、システムの安定性を最大限に保ちながら、スパイクや他の異常を処理する上で重要になります。

このセクションでは、分散展開の利点について説明します。

- ◆ 40 ページのセクション 6.1.1 「追加のコレクタマネージャの利点」
- ◆ 40 ページのセクション 6.1.2 「相関エンジンを追加することの利点」
- ◆ 41 ページのセクション 6.1.3 「追加の NetFlow コレクタマネージャの利点」

6.1.1 追加のコレクタマネージャの利点

Sentinel サーバには、デフォルトでコレクタマネージャが含まれています。ただし運用環境では、コレクタマネージャを分散させることにより、大量のデータを受け取る場合に一層優れた分離を実現できます。こうした状態では、分散されたコレクタマネージャのオーバーロードが生じる可能性があるものの、Sentinel サーバは途切れることなくユーザ要求に応じることができます。

分散ネットワークに複数のコレクタマネージャをインストールすると、次のような利点があります。

- ◆ **システムのパフォーマンスの向上**: コレクタマネージャを追加すると、分散環境でイベントデータを解析および処理できるため、システムのパフォーマンスが向上します。
- ◆ **データのセキュリティの強化およびネットワーク帯域幅要件の低下**: コレクタマネージャがイベントソースと同じ場所にあると、フィルタ、暗号化、およびデータの圧縮を同じソースで実行できます。
- ◆ **ファイルキャッシング**: イベントのアーカイブやイベントの大量発生処理でサーバの負荷が一時的に上がったときに、追加のコレクタマネージャで大量のデータをキャッシュすることができます。この機能は、イベントキャッシングをネイティブでサポートしない Syslog などのプロトコルの場合に役立ちます。

追加のコレクタマネージャをネットワーク内の適切な場所にインストールすることができます。これらのリモートコレクタマネージャはコネクタやコレクタを実行し、収集したデータは Sentinel サーバに転送されて保管、処理されます。追加のコレクタマネージャのインストールについては、[63 ページのパート III 「Sentinel のインストール」](#) を参照してください。

注: 1 つのシステムに複数のコレクタマネージャをインストールすることはできません。リモートシステムに追加のコレクタマネージャをインストールして、それらを Sentinel サーバに接続することはできません。

6.1.2 関連エンジンを追加することの利点

環境設定を複製したり、データベースを追加したりすることなく、複数の関連エンジンをそれぞれ独自のサーバに展開できます。関連ルールが多数ある環境やイベント発生率が極端に高い環境では、複数の関連エンジンをインストールして、新しい関連エンジンにルールを再展開するほうが効率的です。関連エンジンを複数使用すると、Sentinel システムにデータソースが追加された場合やイベント発生率が增大した場合に、それに対応するスケーラビリティが得られます。追加の関連エンジンのインストールについては、[63 ページのパート III 「Sentinel のインストール」](#) を参照してください。

注: 1 つのシステムに複数の関連エンジンをインストールすることはできません。リモートシステムに追加の関連エンジンをインストールして、それらを Sentinel サーバに接続することはできません。

6.1.3 追加の NetFlow コレクタマネージャの利点

NetFlow コレクタマネージャは、ネットワークデバイスからネットワークフローデータを収集します。イベントストレージや検索などの重要な機能のためにシステムリソースを解放するには、Sentinel サーバ上の NetFlow コレクタマネージャを使用するのではなく、追加の NetFlow コレクタマネージャをインストールしてください。

以下のシナリオで追加の NetFlow コレクタマネージャをインストールできます。

- ◆ 多数のネットワークデバイスと大量のネットワークフローデータが存在する環境で、複数の NetFlow コレクタマネージャをインストールして、負荷を分散させることができます。
- ◆ マルチテナント環境の場合、それぞれのテナント用に個別の NetFlow コレクタマネージャをインストールして、テナントごとにネットワークフローデータを収集する必要があります。

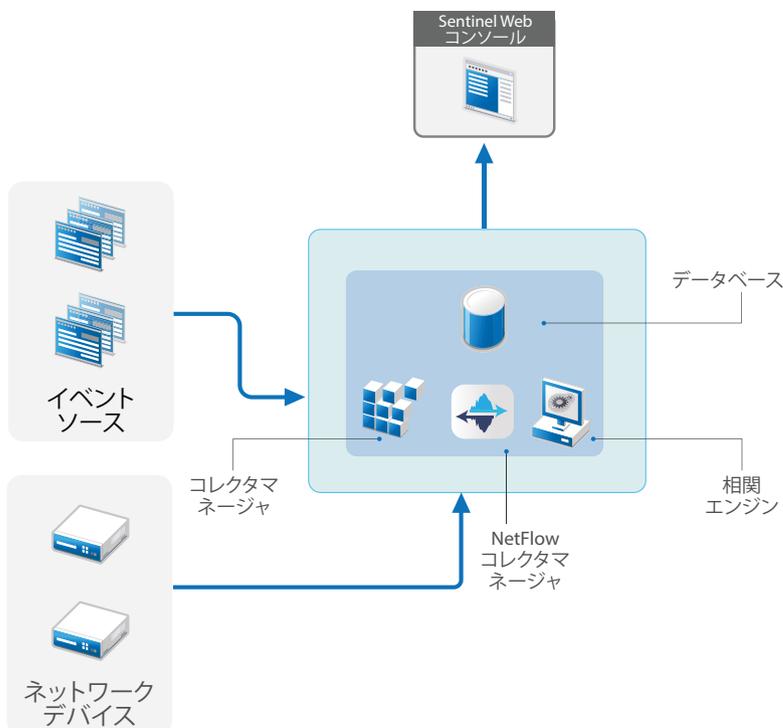
追加の NetFlow コレクタマネージャのインストールについて詳しくは、[89 ページの第 14 章「NetFlow コレクタマネージャのインストール」](#)を参照してください。

6.2 オールインワン展開

最も基本的な展開オプションは、単一のコンピュータ上にすべての Sentinel コンポーネントをインストールするオールインワンシステムです。オールインワン展開は、システムの負荷が小さく、Windows マシンを監視する必要がない場合にのみ適しています。多くの環境では、予測が困難で流動的な負荷や、コンポーネント間のリソースの競合が原因で、パフォーマンスの問題が発生する可能性があります。

重要：運用環境には分散展開をセットアップして、データ収集コンポーネントが個別のコンピュータに分離することをお勧めします。これは、システムの安定性を最大限に保ちながら、スパイクや他の異常を処理する上で重要になります。

図 6-1 オールインワン展開

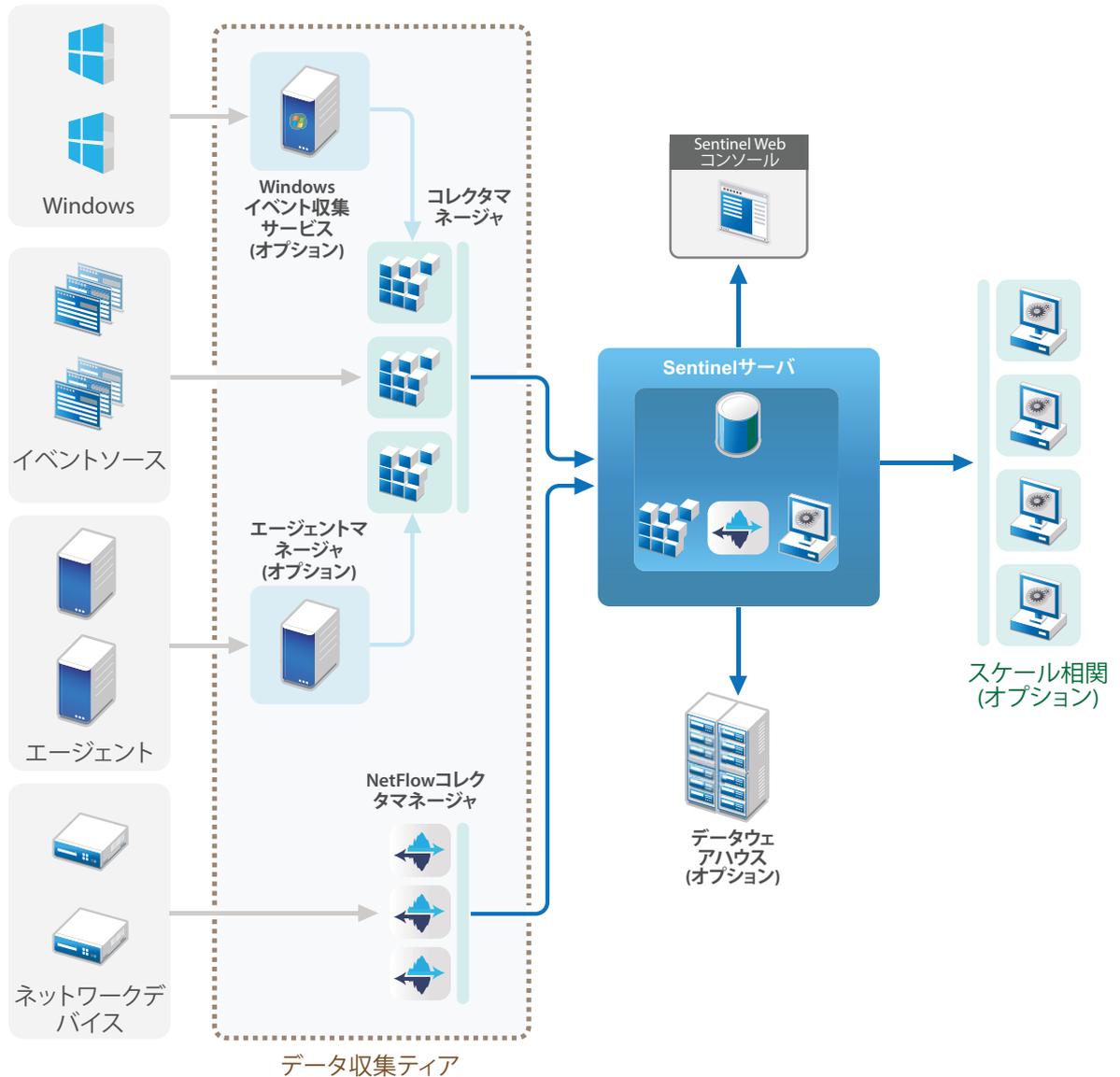


6.3 1 層分散展開

1 層展開は、Windows コンピュータを監視できるだけでなく、オールインワン展開よりも大きな負荷を処理できます。コレクタマネージャ、NetFlow コレクタマネージャ、および相関エンジンのコンピュータを追加して、中央 Sentinel サーバの処理をオフロードすることで、データの収集と相関をスケールアウトできます。また、イベント、相関ルール、およびネットワークフローデータの負荷の処理に加えて、リモートのコレクタマネージャ、相関エンジン、NetFlow コレクタマネージャは、イベントの保存や検索などの他の要求に対処するために中央 Sentinel サーバ上のリソースを解放します。システムの負荷が増えるにつれ、中央 Sentinel サーバが最終的にボトルネックになってきたら、展開の階層を増やしてさらにスケールアウトする必要があります。

オプションで、イベントデータをデータウェアハウスにコピーするように Sentinel を構成できます。この方法は、カスタムレポート、分析、およびその他の処理を別のシステムにオフロードする場合に便利です。

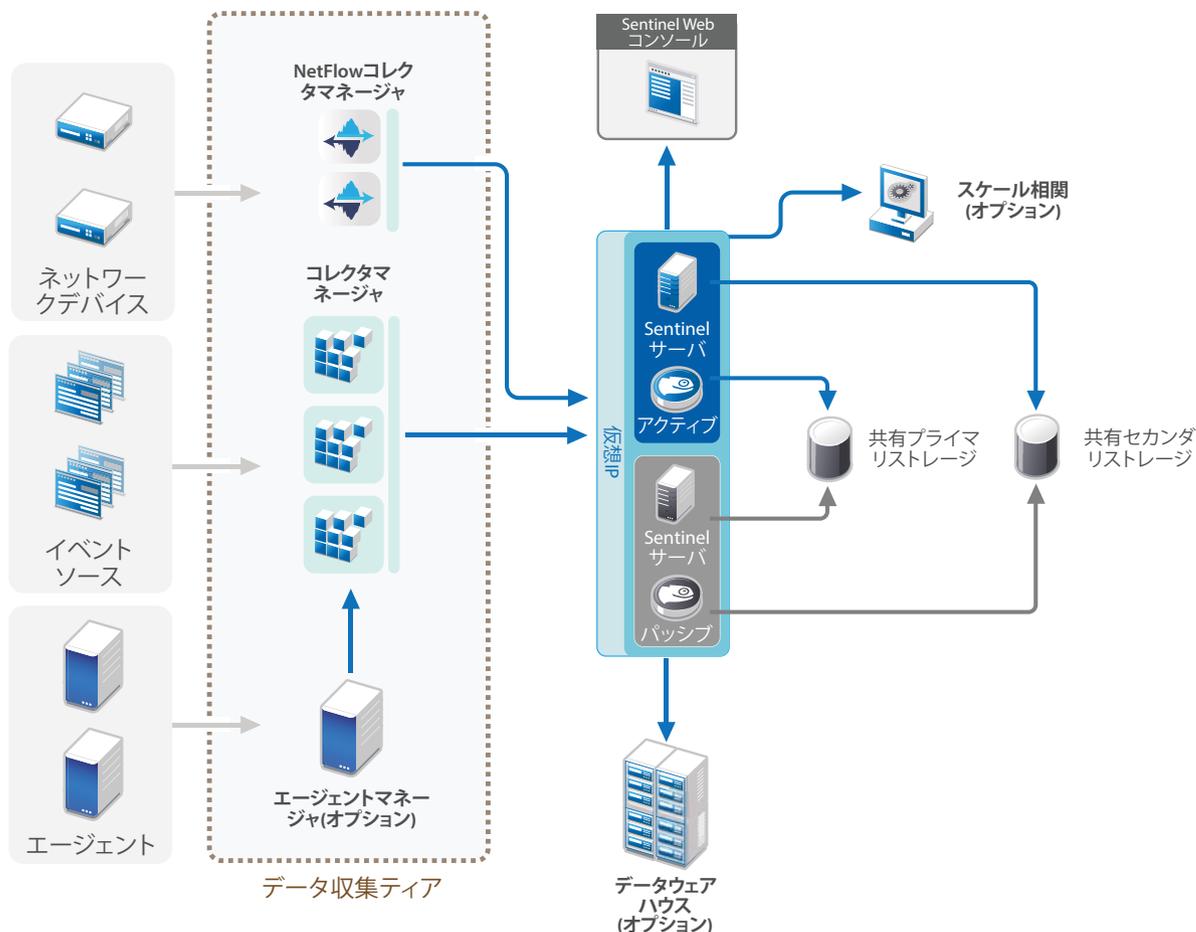
図 6-2 1 層分散展開



6.4 高可用性を備えた 1 層分散展開

この 1 層分散展開は、いかにフェールオーバー冗長性を備えた高可用性システムに変化できるかを示しています。高可用性での Sentinel の展開について詳しくは、143 ページのパート VI「高可用性のための Sentinel の展開」を参照してください。

図 6-3 高可用性を備えた 1 層分散展開

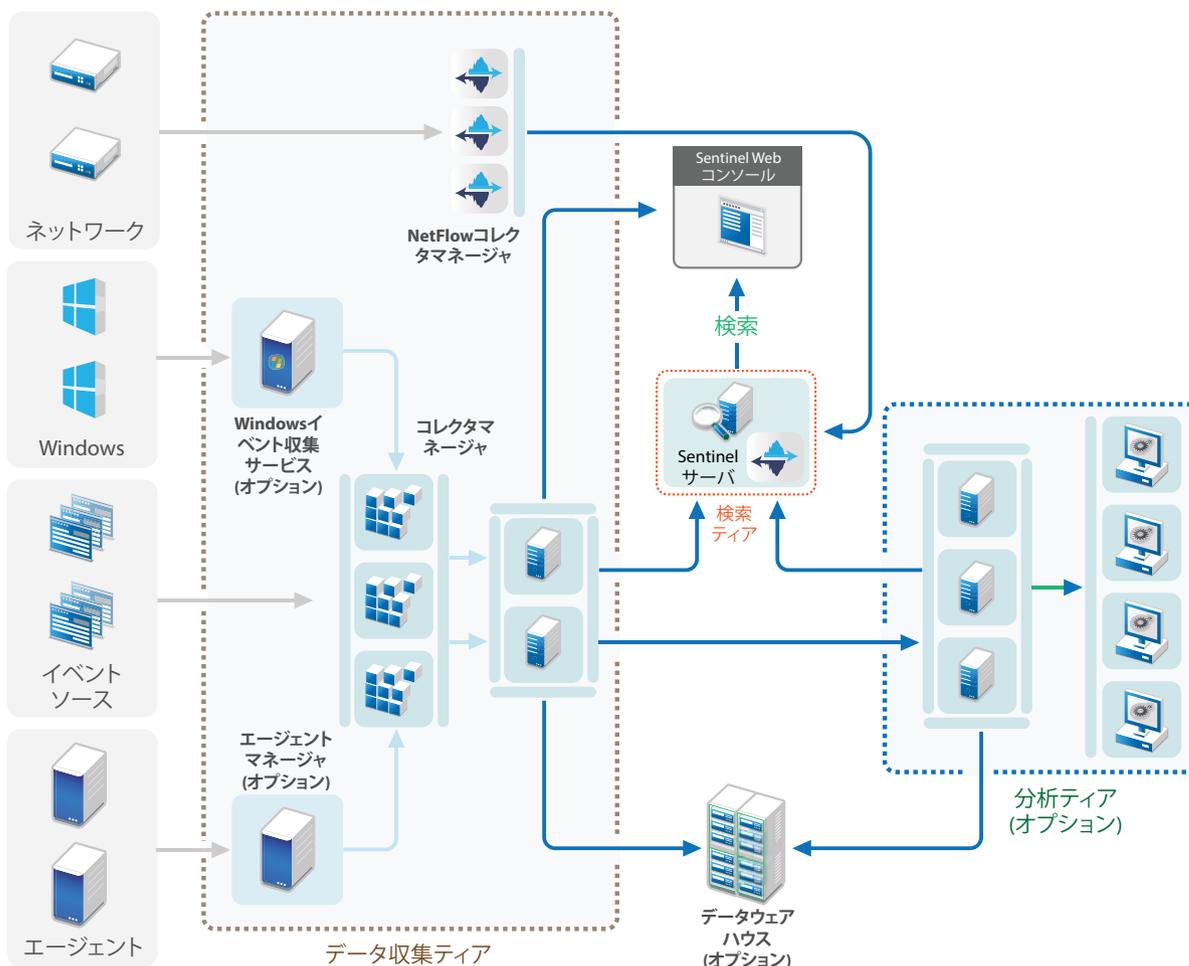


6.5 2 層および 3 層分散展開

この展開では、Sentinel リンク機能と Sentinel データフェデレーション機能を活用することで、単一の中央 Sentinel サーバの負荷処理能力を超えて、処理負荷を複数の Sentinel インスタンスで共有できるようになります。データ収集層で示したように、データ収集はそれぞれで複数のコレクタマネージャが動作する複数の Sentinel サーバによって負荷分散されています。イベント関連またはセキュリティインテリジェンスを実現したい場合は、オプションで、Sentinel Link を使ってデータを分析層に転送できます。検索層は Sentinel データフェデレーションを使用することで、すべての別階層にあるシステムをすべて検索できる、便利な単一アクセスポイントを提供します。検索要求が Sentinel の複数のインスタンスで共有されるため、この展開は検索負荷分散特性も備えています。この特性は、大規模な検索負荷を処理するためのスケーリングに役立ちます。

ネットワークフローデータは検索層に保存されます。これにより、検索結果からコンテキストネットワークトラフィック分析へ簡単に進むことができます。

図 6-4 2 層および 3 層分散展開



6.6 データストレージのパーティション計画

Sentinel をインストールするときに、Sentinel のインストール先 (デフォルトでは /var/opt/novell ディレクトリ) に、プライマリストレージ用のディスクパーティションをマウントする必要があります。

ディスク使用量が正しく計算されるように、/var/opt/novell/sentinel ディレクトリの下ディレクトリ構造全体が、1つのディスクパーティションに置かれている必要があります。そうしないと、自動データ管理機能がイベントデータを途中で削除してしまう可能性があります。Sentinel ディレクトリ構造の詳細については、[47 ページのセクション 6.6.4 「Sentinel のディレクトリ構造」](#) を参照してください。

ベストプラクティスとして、このデータディレクトリが、実行可能ファイル、環境設定ファイル、オペレーティングシステムファイルとは別のディスクパーティションに配置されるようにしてください。可変データを別に保存することには、一連のファイルのバックアップが容易になり、破損した場合の回復が簡単になるというメリットがあるうえ、ディスクパーティションが満杯になった場合の堅牢性が向上します。また、容量の小さいファイルシステムのほうが効率的であるため、システム全体のパフォーマンスも向上します。詳細については、「[Disk partitioning](#)」を参照してください。

注：ファイルストレージとしての ext3 ファイルシステムには制限があります。32000 を超えるファイルまたはサブディレクトリを、1つのディレクトリで保持することはできません。多数の保存ポリシーを用意する予定がある場合や、データを長期間（たとえば、1年間）保持する予定がある場合は、XFS ファイルシステムの使用をお勧めします。

6.6.1 従来型インストールでのパーティションの使用

従来型インストールの場合は、Sentinel をインストールする前にオペレーティングシステムのディスクパーティションレイアウトを変更できます。管理者は [47 ページのセクション 6.6.4 「Sentinel のディレクトリ構造」](#) で説明されているディレクトリ構造に基づいて、適切なディレクトリに目的のパーティションを作成およびマウントする必要があります。インストーラを実行すると Sentinel は事前に作成されたディレクトリにインストールされ、複数のパーティションにわたるインストール環境が構築されます。

注：

- ◆ インストーラの実行中に `--location` オプションを使用して、ファイルを格納する場所としてデフォルトのディレクトリ以外の最上位の場所を指定できます。`--location` オプションに渡す値は、ディレクトリパスの前に付加されます。たとえば、「`--location=/foo`」を指定すると data ディレクトリは `/foo/var/opt/novell/sentinel/data`、config ディレクトリは `/foo/etc/opt/novell/sentinel/config` となります。
 - ◆ `--location` オプションには、ファイルシステムリンク（ソフトリンクなど）は使用しないでください。
-

6.6.2 アプライアンスインストールでのパーティションの使用

DVD ISO アプライアンスフォーマットを使用している場合、YaST 画面の指示に従って、インストール中にアプライアンスのファイルシステムのパーティション化を設定できます。たとえば、`/var/opt/novell/sentinel` マウントポイントに別のパーティションを作成して、すべてのデータを別のパーティションに置くことができます。ただし、他のアプライアンスフォーマットの場合は、インストール後にのみパーティション作成を設定することができます。SuSE YaST システム環境設定ツールを使用して、パーティションを追加し、その新しいパーティションにディレクトリを移動することができます。インストール後のパーティション作成の詳細については、[84 ページのセクション 13.3.2 「パーティションの作成」](#) を参照してください。

6.6.3 パーティションレイアウトのベストプラクティス

多くの組織が、独自に、インストールしたシステムに関するベストプラクティスパーティションレイアウトスキームを文書化しています。以下のパーティション提案の目的は、定義済みのポリシーを持たない組織をガイドし、Sentinel 固有のファイルシステムの使い方を考慮することです。概して、Sentinel は可能な範囲で [ファイルシステム階層基準](#) に準拠しています。

パーティション	マウントポイント	サイズ	備考
ルート	/	100GB	オペレーティングシステムファイルと Sentinel バイナリ / 環境設定が保存されます。

パーティション	マウントポイント	サイズ	備考
ブート	/boot	150MB	ブートパーティション
一時	/tmp	30GB	OS ファイルと Sentinel 一時ファイル用の場所。この場所を別のパーティションに隔離することによって、暴走プロセスが一時領域を使い果たしてもアプリケーションデータは破損から保護されます。
プライマリストレージ	/var/opt/novell/sentinel	System Sizing Information を使用して計算します。	この領域には、プライマリ Sentinel 収集データと、その他の可変データ (ログファイルなど) が保存されます。このパーティションは他のシステムと共有できます。
セカンダリストレージ	ストレージのタイプ (NFS、CIFS、または SAN) に基づく場所。	System Sizing Information を使用して計算します。	これはセカンダリストレージ領域で、前述のようにローカルにマウントすることも、リモートでマウントすることもできます。
アーカイバルストレージ	リモートシステム	System Sizing Information を使用して計算します。	このストレージはアーカイブしたデータ用です。

6.6.4 Sentinel のディレクトリ構造

デフォルトでは、Sentinel のディレクトリは次の場所にあります。

- ◆ データファイルは、/var/opt/novell/sentinel/data ディレクトリおよび /var/opt/novell/sentinel/3rdparty ディレクトリにあります。
- ◆ 実行ファイルおよびライブラリは /opt/novell/sentinel ディレクトリに保存されています。
- ◆ ログファイルは、/var/opt/novell/sentinel/log ディレクトリにあります。
- ◆ 環境設定ファイルは、/etc/opt/novell/sentinel ディレクトリにあります。
- ◆ プロセス ID (PID) ファイルは、/var/run/sentinel/server.pid ディレクトリにあります。

PID を使用すると、管理者は Sentinel サーバの親プロセスを識別し、プロセスを監視または終了することができます。

7 FIPS140-2 モードでの展開に関する考慮事項

オプションとして、内部暗号化などの機能に FIPS 140-2 認定暗号プロバイダである Mozilla ネットワークセキュリティサービス (NSS) を使用するように、Sentinel を設定することができます。この目的は、Sentinel を「FIPS 140-2 実装」にして、米国連邦購入ポリシーおよび標準に準拠させることです。

Sentinel の FIPS 140-2 モードを有効にすると、Sentinel サーバ、Sentinel リモートコレクタマネージャ、Sentinel リモート相関エンジン、Sentinel Web インタフェース、Sentinel コントロールセンター、および Sentinel Advisor サービスとの通信に、FIPS 140-2 認定暗号が使用されます。

- ◆ [49 ページのセクション 7.1 「Sentinel における FIPS 実装」](#)
- ◆ [50 ページのセクション 7.2 「Sentinel の FIPS 実装コンポーネント」](#)
- ◆ [51 ページのセクション 7.3 「実装チェックリスト」](#)
- ◆ [52 ページのセクション 7.4 「導入シナリオ」](#)

7.1 Sentinel における FIPS 実装

Sentinel は、オペレーティングシステムによって提供される Mozilla NSS ライブラリを使用します。Red Hat Enterprise Linux (RHEL) と SUSE Linux Enterprise Server (SLES) とでは、付属する NSS パッケージセットが異なります。

RHEL 6.3 によって提供される NSS 暗号化モジュールは、FIPS 140-2 認定です。SLES 11 SP3 によって提供される NSS 暗号化モジュールは、まだ公式には FIPS 140-2 認定ではありませんが、SUSE モジュールを FIPS 140-2 認定にするための作業が進行中です。認定が取得されれば、SUSE プラットフォームで「FIPS 140-2 実装」にするために Sentinel に変更を加える必要はありません。

RHEL 6.2 FIPS 140-2 証明書の詳細については、『[Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules](#)』を参照してください。

7.1.1 RHEL NSS パッケージ

FIPS 140-2 モードに対応するために、Sentinel には次の 64 ビット NSS パッケージが必要です。

- ◆ nspr-4.9-1.el6.x86_64
- ◆ nss-sysinit-3.13.3-6.el6.x86_64
- ◆ nss-util-3.13.3-2.el6.x86_64
- ◆ nss-softokn-freebl-3.12.9-11.el6.x86_64
- ◆ nss-softokn-3.12.9-11.el6.x86_64
- ◆ nss-3.13.3-6.el6.x86_64
- ◆ nss-tools-3.13.3-6.el6.x86_64

上記のパッケージでインストールされていないものがあれば、それらをインストールしてから Sentinel の FIPS 140-2 モードを有効にする必要があります。

7.1.2 SLES NSS パッケージ

FIPS 140-2 モードに対応するために、Sentinel には次の 64 ビット NSS パッケージが必要です。

- ◆ libfreebl3-3.13.1-0.2.1
- ◆ mozilla-nspr-4.8.9-1.2.2.1
- ◆ mozilla-nss-3.13.1-0.2.1
- ◆ mozilla-nss-tools-3.13.1-0.2.1

上記のパッケージでインストールされていないものがあれば、それらをインストールしてから Sentinel の FIPS 140-2 モードを有効にする必要があります。

7.2 Sentinel の FIPS 実装コンポーネント

次の Sentinel コンポーネントは FIPS 140-2 に対応しています。

- ◆ すべての Sentinel プラットフォームコンポーネントは、FIPS 140-2 モードをサポートするように更新されています。
- ◆ 暗号化をサポートする以下の Sentinel プラグインは、FIPS 140-2 モードをサポートするように更新されています。
 - ◆ エージェントマネージャコネクタ 2011.1r1 以降
 - ◆ データベース (JDBC) コネクタ 2011.1r2 以降
 - ◆ ファイルコネクタ 2011.1r1 以降 (イベントソースタイプがローカルまたは NFS の場合のみ)
 - ◆ LDAP インテグレーター 2011.1r1 以降
 - ◆ Sentinel Link コネクタ 2011.1r3 以降
 - ◆ Sentinel Link インテグレーター 2011.1r2 以降
 - ◆ SMTP インテグレーター 2011.1r1 以降
 - ◆ Syslog コネクタ 2011.1r2 以降
 - ◆ Windows イベント (WMI) コネクタ 2011.1r2 以降
 - ◆ チェックポイント (LEA) コネクタ 2011.1r2 以降

上記の Sentinel プラグインを FIPS 140-2 モードで実行するための環境設定については、[112 ページの「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」](#)を参照してください。

本書のリリース時点で、オプションの暗号化をサポートする以下の Sentinel コネクタは、まだ FIPS 140-2 モードをサポートするように更新されていません。ただし、これらのコネクタを使用したイベントの収集は引き続き実行することができます。これらのコネクタを FIPS 140-2 モードの Sentinel で使用する方法の詳細については、[117 ページの「FIPS 140-2 モードの Sentinel で FIPS 非対応コネクタを使用する」](#)を参照してください。

- ◆ Cisco SDEE コネクタ 2011.1r1

- ◆ ファイルコネクタ 2011.1r1 (CIFS および SCP 機能には暗号化が含まれていますが、FIPS 140-2 モードでは動作しません)。
- ◆ NetIQ Audit Connector 2011.1r1
- ◆ SNMP Connector 2011.1r1

本書のリリース時点で、SSL をサポートする以下の Sentinel インテグレータは、FIPS 140-2 モードをサポートするように更新されていません。ただし、これらのインテグレータを FIPS 140-2 モードの Sentinel で使用している場合でも、非暗号化接続は継続して使用できます。

- ◆ Remedy インテグレータ 2011.1r1 以降
- ◆ SOAP インテグレータ 2011.1r1 以降

上記のリストに含まれていない Sentinel プラグインはどれも暗号化を使用せず、Sentinel を FIPS 140-2 モードにしたことによる影響を受けません。それらを FIPS 140-2 モードの Sentinel で使用するために、追加ステップを実行する必要はありません。

Sentinel プラグインの詳細については、[Sentinel プラグイン Web サイト](#)をご覧ください。まだ更新されていないプラグインを FIPS に対応させたい場合は、[Bugzilla](#) を使用してリクエストを送信してください。

7.3 実装チェックリスト

次の表は、Sentinel を FIPS 140-2 モードで運用するために必要なタスクの概要を示しています。

タスク	詳細の参照先
展開を計画する。	52 ページのセクション 7.4 「導入シナリオ」
FIPS 140-2 モードを、Sentinel のインストール中に有効にするか、後から有効にするかを定める。 インストール中に Sentinel の FIPS 140-2 モードを有効にする場合、インストールの処理中にカスタムインストールかサイレントインストールを選択する必要があります。	71 ページのセクション 12.2.2 「Sentinel サーバのカスタムインストール」 75 ページのセクション 12.3 「サイレントインストールの実行」 107 ページの第 20 章 「既存の Sentinel インストール環境を FIPS 140-2 モードにする」
Sentinel プラグインを FIPS 140-2 モードで実行するように設定する。	112 ページのセクション 21.5 「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」
証明書を Sentinel FIPS キーストアにインポートする。	118 ページのセクション 21.6 「証明書を FIPS キーストアデータベースにインポートする」

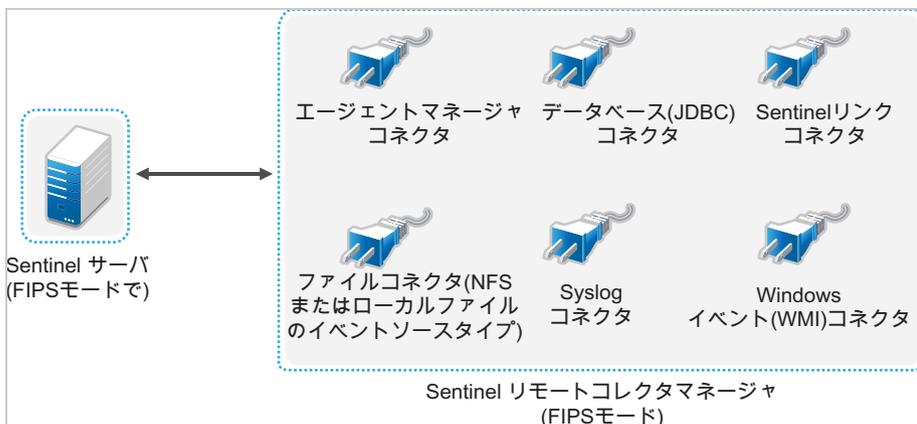
注：FIPS モードへの変換を開始する前に、Sentinel システムのバックアップを取ることを強くお勧めします。後でサーバを非 FIPS モードに戻す必要がある場合、サポートされている方法はバックアップからの復元のみになります。非 FIPS モードへ戻す方法について詳しくは、[118 ページの「Sentinel を非 FIPS モードに戻す」](#)を参照してください。

7.4 導入シナリオ

このセクションでは、Sentinel の FIPS 140-2 モードの導入シナリオについて説明します。

7.4.1 シナリオ 1: 完全 FIPS 140-2 モードでのデータ収集

このシナリオの場合、データ収集は FIPS 140-2 モードをサポートするコネクタによってのみ実行されます。Sentinel サーバがあり、リモートコレクタマネージャによってデータが収集されている環境を前提としています。リモートコレクタマネージャは、1 つまたは複数を使用することができます。



ご使用の環境で FIPS 140-2 モードをサポートするコネクタのみを使用してイベントソースからデータ収集が行われている場合は、以下の手順を実行する必要があります。

- 1 FIPS 140-2 モードの Sentinel サーバが必要です。

注: 新規インストールまたはアップグレードされた Sentinel サーバが非 FIPS モードである場合は、Sentinel サーバの FIPS を有効にする必要があります。詳細については、[107 ページの「Sentinel サーバを FIPS 140-2 モードで実行する」](#)を参照してください。

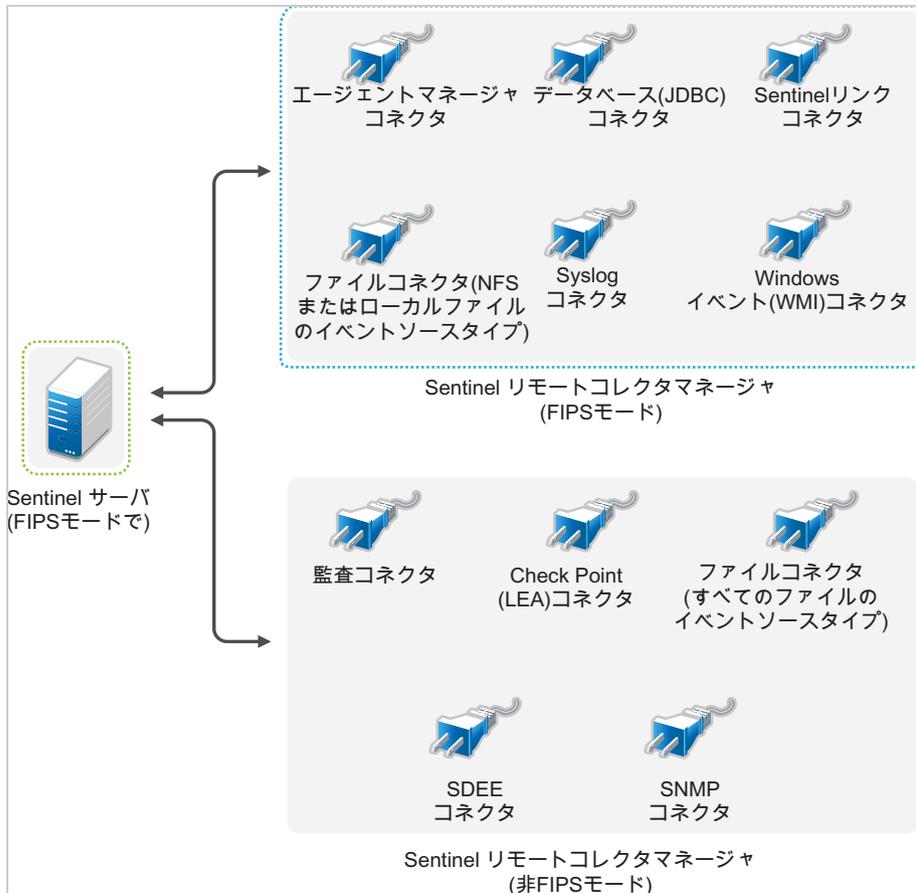
- 2 Sentinel リモートコレクタマネージャを FIPS 140-2 モードで実行させておく必要があります。

注: 新規インストールまたはアップグレードされたリモートコレクタマネージャが非 FIPS モードで実行中である場合は、リモートコレクタマネージャの FIPS を有効にする必要があります。詳細については、[107 ページの「リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする」](#)を参照してください。

- 3 FIPS サーバとリモートコレクタマネージャが相互に通信していることを確認します。
- 4 リモート関連エンジンがある場合は、それらを FIPS モードで実行するように変換します。詳細については、[107 ページの「リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする」](#)を参照してください。
- 5 Sentinel プラグインを FIPS 140-2 モードで実行するように設定します。詳細については、[112 ページの「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」](#)を参照してください。

7.4.2 シナリオ 2: 部分 FIPS 140-2 モードでのデータ収集

このシナリオの場合、データ収集は FIPS 140-2 モードをサポートするコネクタと FIPS 140-2 モードをサポートしないコネクタを使用して実行されます。ここでは、データはリモートコレクタマネージャによって収集されると仮定します。リモートコレクタマネージャは、1つまたは複数を使用することができます。



FIPS 140-2 モードをサポートするコネクタとサポートしないコネクタを使用してデータ収集を処理する場合、2つのリモートコレクタマネージャを使用する必要があります。1つは FIPS をサポートするコネクタ用に FIPS 140-2 モードで実行し、もう 1つは FIPS 140-2 モードをサポートしないコネクタ用に非 FIPS (通常) モードで実行します。

FIPS 140-2 モードをサポートしているコネクタと、FIPS 140-2 モードをサポートしていないコネクタを使用して、イベントソースからデータを収集している環境では、以下の手順を実行する必要があります。

- 1 FIPS 140-2 モードの Sentinel サーバが必要です。

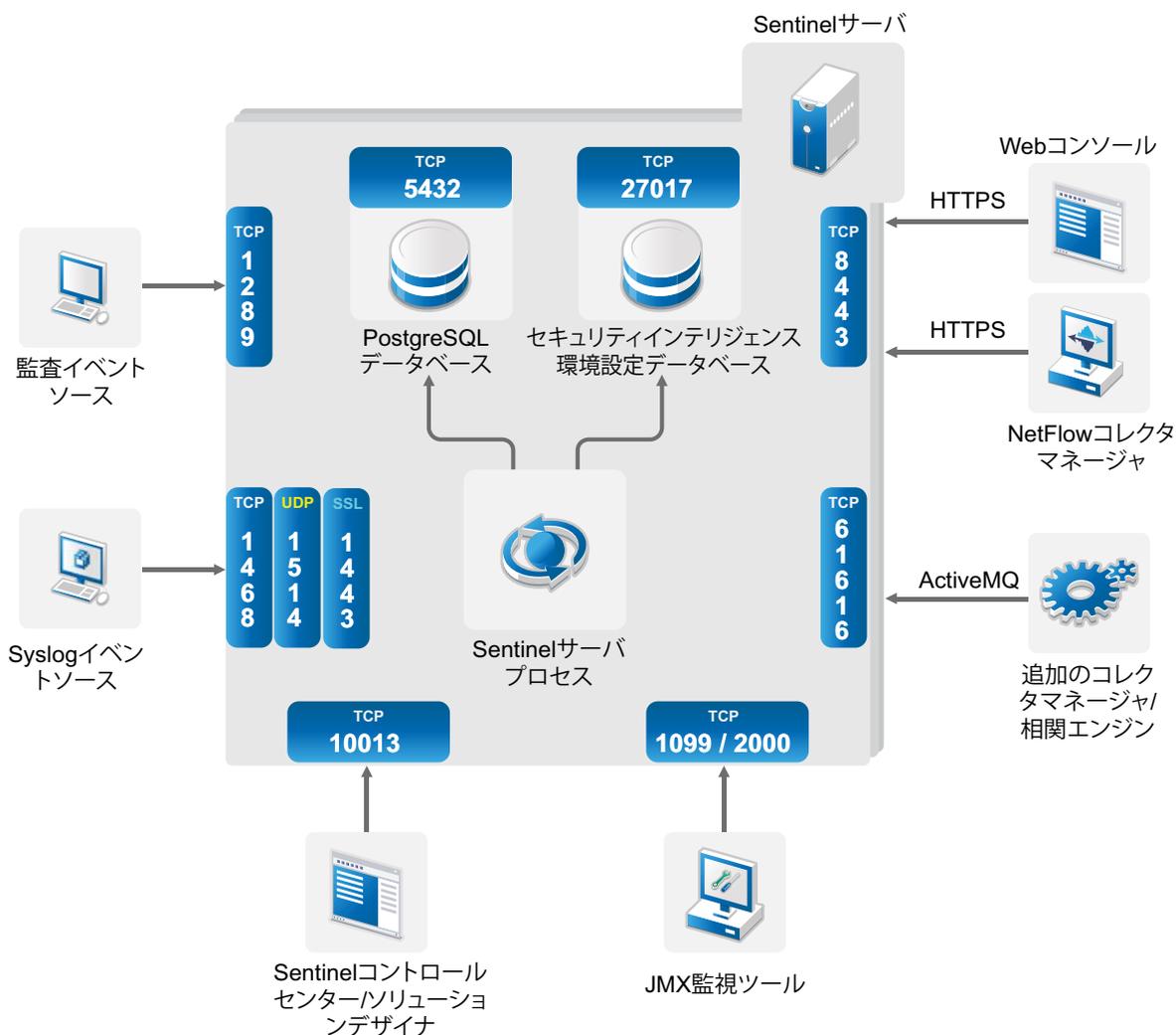
注: 新規インストールまたはアップグレードされた Sentinel サーバが非 FIPS モードである場合は、Sentinel サーバの FIPS を有効にする必要があります。詳細については、[107 ページの「Sentinel サーバを FIPS 140-2 モードで実行する」](#)を参照してください。

- 2 1つのリモートコレクタマネージャは FIPS 140-2 モードで実行し、もう1つのリモートコレクタマネージャは引き続き非 FIPS モードで実行してください。
 - 2a FIPS 140-2 モード有効のリモートコレクタマネージャがない場合は、リモートコレクタマネージャで FIPS モードを有効にする必要があります。詳細については、[107 ページの「リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする」](#)を参照してください。
 - 2b FIPS 非対応リモートコレクタマネージャのサーバ証明書を更新します。詳細については、[111 ページの「リモートコレクタマネージャおよび関連エンジンのサーバ証明書の更新」](#)を参照してください。
- 3 2つのリモートコレクタマネージャが FIPS 140-2 対応の Sentinel サーバと通信していることを確認します。
- 4 リモート関連エンジンがある場合は、それらを FIPS 140-2 モードで実行するように設定します。詳細については、[107 ページの「リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする」](#)を参照してください。
- 5 Sentinel プラグインを FIPS 140-2 モードで実行されるように環境設定します。詳細については、[112 ページの「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」](#)を参照してください。
 - 5a FIPS 140-2 モードをサポートするコネクタを、FIPS モードで実行するリモートコレクタマネージャに展開します。
 - 5b FIPS 140-2 モードをサポートしないコネクタを、非 FIPS のリモートコレクタマネージャに展開します。

8 使用するポート

Sentinel は、さまざまなポートを使用して、他のコンポーネントとの外部通信を行います。アプリケーションをインストールするため、ポートはファイアウォール上でデフォルトで開かれています。ただし、従来型インストールでは、Sentinel のインストール先となるオペレーティングシステムで、ファイアウォールのポートを開く設定を行う必要があります。Sentinel で使用するポートを次の図に示します。

図 8-1 Sentinel で使用するポート



- ◆ 56 ページのセクション 8.1 「Sentinel サーバのポート」
- ◆ 58 ページのセクション 8.2 「コレクタマネージャのポート」
- ◆ 59 ページのセクション 8.3 「関連エンジンのポート」
- ◆ 60 ページのセクション 8.4 「NetFlow コレクタマネージャのポート」

8.1 Sentinel サーバのポート

Sentinel サーバは、内部通信と外部通信に次のポートを使用します。

8.1.1 ローカルポート

Sentinel は、データベースや他の内部プロセスとの内部通信に次のポートを使用します。

ポート	説明
TCP 27017	セキュリティインテリジェンス環境設定データベースで使用されます。
TCP 28017	セキュリティインテリジェンスデータベースの Web インタフェースで使用されます。
TCP 32000	ラッパープロセスとサーバプロセス間の内部通信で使用されます。
TCP 9200	REST を使用したアラートのインデックス作成サービスとの通信で使用されます。
TCP 9300	ネイティブプロトコルを使用したアラートのインデックス作成サービスとの通信で使用されます。

8.1.2 ネットワークポート

Sentinel が正常に動作するように、次のポートがファイアウォール上で開かれていることを確認してください。

ポート	方向	必須 / オプション	説明
TCP 5432	INBOUND	オプション。	PostgreSQL データベースで使用されます。デフォルトでは、このポートはループバックインタフェースのみをリスンします。
TCP 1099 および 2000	INBOUND	オプション	監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。
TCP 1289	INBOUND	オプション	Audit の接続用に使用されます。
UDP 1514	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 8443	INBOUND	必須	HTTPS 通信および NetFlow コレクタマネージャからの着信接続に使用されます。
TCP 1443	INBOUND	オプション	SSL で暗号化された Syslog メッセージに使用されます。
TCP 61616	INBOUND	オプション	コレクタマネージャおよび関連エンジンからの着信接続に使用されます。
TCP 10013	INBOUND	必須	Sentinel コントロールセンターおよびソリューションデザイナーが使用します。

ポート	方向	必須 / オプション	説明
TCP 1468	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 10014	INBOUND	オプション	リモートのコレクタマネージャにより、SSL プロキシを介してサーバに接続するのに使用されます。ただし、これは一般的ではありません。デフォルトでは、リモートのコレクタマネージャは SSL ポート 61616 を使用してサーバに接続します。
TCP 443	OUTBOUND	オプション	Advisor が使用されている場合は、このポートがインターネットを経由して Advisor Updates ページ につながる Advisor サービスへの接続を開始します。
TCP 8443	OUTBOUND	オプション	データフェデレーションが使用されている場合は、分散検索を実行するために、このポートが別の Sentinel システムへの接続を開始します。
TCP 389 または 636	OUTBOUND	オプション	LDAP 認証が使用されると、このポートが LDAP サーバへの接続を開始します。
TCP/UDP 111 および TCP/UDP 2049	OUTBOUND	オプション	セカンダリストレージが NFS を使用するように設定されている場合。
TCP 137、138、139、445	OUTBOUND	オプション	セカンダリストレージが CIFS を使用するように設定されている場合。
TCP JDBC (データベース依存)	OUTBOUND	オプション	データ同期が使用されると、このポートが JDBC を使用するターゲットデータベースへの接続を開始します。使用されるポートはターゲットデータベースによって異なります。
TCP 25	OUTBOUND	オプション	電子メールサーバへの接続を開始します。
TCP 1290	OUTBOUND	オプション	Sentinel がイベントを別の Sentinel システムに転送すると、このポートがそのシステムへの Sentinel Link 接続を開始します。
UDP 162	OUTBOUND	オプション	Sentinel が SNMP トラップを受信するシステムにイベントを転送すると、このポートがパケットを受信者に送信します。
UDP 514 または TCP 1468	OUTBOUND	オプション	このポートは、Sentinel が Syslog メッセージを受信するシステムにイベントを転送するときに使用されます。このポートが UDP である場合は、パケットを受信者に送信します。このポートが TCP である場合は、受信者への接続を開始します。

8.1.3 Sentinel サーバアプライアンス固有のポート

上記のポートに加えて、アプライアンス用に次のポートが開いています。

ポート	方向	必須 / オプション	説明
TCP 22	INBOUND	必須	シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。
TCP 4984	INBOUND	必須	Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。
TCP 289	INBOUND	オプション	Audit 接続用の 1289 に転送されます。
TCP 443	INBOUND	オプション	HTTPS 通信用に 8443 に転送されます。
UDP 514	INBOUND	オプション	Syslog メッセージ用に 1514 に転送されます。
TCP 1290	INBOUND	オプション	SuSE Firewall を抜けて接続することが許可されている Sentinel Link ポート。
UDP および TCP 40000 - 41000	INBOUND	オプション	syslog などのデータ収集サーバの設定に使用可能なポートです。Sentinel は、これらのポートをデフォルトではリスンしません。
TCP 443 または 80	OUTBOUND	必須	インターネット上の NetIQ アプライアンスソフトウェアアップデートリポジトリ、またはネットワーク内の Subscription Management Tool サービスへの接続を開始します。
TCP 80	OUTBOUND	オプション	Subscription Management Tool への接続を開始します。

8.2 コレクタマネージャのポート

コレクタマネージャは、以下のポートを使用して他のコンポーネントと通信します。

8.2.1 ネットワークポート

Sentinel コレクタマネージャが正常に動作できるよう、ファイアウォール上で次のポートが開かれていることを確認してください。

ポート	方向	必須 / オプション	説明
TCP 1289	INBOUND	オプション	Audit の接続用に使用されます。
UDP 1514	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 1443	INBOUND	オプション	SSL で暗号化された Syslog メッセージに使用されます。
TCP 1468	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 1099 および 2000	INBOUND	オプション	監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されません。

ポート	方向	必須 / オプション	説明
TCP 61616	OUTBOUND	必須	Sentinel サーバへの接続を開始します。

8.2.2 コレクタマネージャアプライアンス固有のポート

上記のポートに加えて、Sentinel コレクタマネージャアプライアンス用に次のポートが開いています。

ポート	方向	必須 / オプション	説明
TCP 22	INBOUND	必須	シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。
TCP 4984	INBOUND	必須	Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。
TCP 289	INBOUND	オプション	Audit 接続用の 1289 に転送されます。
UDP 514	INBOUND	オプション	Syslog メッセージ用に 1514 に転送されます。
TCP 1290	INBOUND	オプション	SuSE Firewall を介した接続が許可される Sentinel リンクポートです。
UDP および TCP 40000 - 41000	INBOUND	オプション	データ収集サーバ (syslog など) を設定するときに使用します。Sentinel は、これらのポートをデフォルトではリスンしません。
TCP 443	OUTBOUND	必須	インターネット上の NetIQ アプライアンスソフトウェア アップデトリポジトリ、またはネットワーク内の Subscription Management Tool サービスへの接続を開始します。
TCP 80	OUTBOUND	オプション	Subscription Management Tool への接続を開始します。

8.3 関連エンジンのポート

関連エンジンは、以下のポートを使用して他のコンポーネントと通信します。

8.3.1 ネットワークポート

Sentinel 関連エンジンが正常に動作するように、ファイアウォール上で次のポートが開かれていることを確認してください。

ポート	方向	必須 / オプション	説明
TCP 1099 および 2000	INBOUND	オプション	監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。

ポート	方向	必須 / オプション	説明
TCP 61616	OUTBOUND	必須	Sentinel サーバへの接続を開始します。

8.3.2 関連エンジンアプライアンス固有のポート

Sentinel 関連エンジンアプライアンスでは、上記のポートに加えて次のポートが開いています。

ポート	方向	必須 / オプション	説明
TCP 22	INBOUND	必須	シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。
TCP 4984	INBOUND	必須	Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。
TCP 443	OUTBOUND	必須	インターネット上の NetIQ アプライアンスソフトウェアアップデートリポジトリ、またはネットワーク内の Subscription Management Tool サービスへの接続を開始します。
TCP 80	OUTBOUND	オプション	Subscription Management Tool への接続を開始します。

8.4 NetFlow コレクタマネージャのポート

NetFlow コレクタマネージャは、以下のポートを使用して他のコンポーネントと通信します。

ポート	方向	必須 / オプション	説明
HTTPS 8443	OUTBOUND	必須	Sentinel サーバへの接続を開始します。
3578	INBOUND	必須	ネットワークデバイスからネットワークフローデータを受信するために使用します。

9 インストールオプション

Sentinel の従来型インストールを実行するか、アプライアンスをインストールできます。この章では、次の2つのインストールオプションについて説明します。

9.1 従来型インストール

従来型インストールでは、アプリケーションインストーラを使用して、既存のオペレーティングシステムに Sentinel がインストールされます。次の方法で Sentinel をインストールすることができます。

- ◆ **Interactive:** ユーザの入力によってインストールを進行します。インストール中に、インストールオプション (ユーザ入力またはデフォルト値) をファイルに記録し、それを後でサイレントインストールに使用することができます。標準インストールまたはカスタムインストールのどちらかを実行できます。

標準インストール	カスタムインストール
環境設定にデフォルト値を使用します。ユーザ入力は、パスワードについてのみ必要です。	環境設定セットアップの値を指定するようプロンプトが表示されます。ユーザはデフォルト値を選択するか、または必要な値を指定できます。
デフォルトの評価版キーを使用してインストールします。	デフォルトの評価版ライセンスキーまたは有効なライセンスキーを使用してインストールできます。
管理者パスワードを指定し、その管理者パスワードを dbauser と appuser の両方に対するデフォルトパスワードとして使用できます。	管理者パスワードを指定できます。dbauser と appuser については、新しいパスワードを指定することも、管理者パスワードを使用することもできます。
すべてのコンポーネントに対してデフォルトポートをインストールします。	コンポーネント別にポートを指定できます。
Sentinel を非 FIPS モードでインストールします。	Sentinel を FIPS 140-2 モードでインストールできません。
内部データベースでユーザを認証します。	データベース認証に加えて、Sentinel の LDAP 認証を設定するオプションが提供されます。Sentinel の LDAP 認証の環境設定を行うと、ユーザは Novell eDirectory または Microsoft Active Directory の資格情報を使用してサーバにログインすることができます。

インタラクティブインストールの詳細については、[70 ページのセクション 12.2 「インタラクティブインストールの実行」](#) を参照してください。

- ◆ **サイレント:** 複数の Sentinel サーバをインストールして展開する場合は、標準またはカスタムのインストール中に、環境設定ファイルにインストールオプションを記録し、そのファイルを使用してサイレントインストールを実行することができます。サイレントインストールの詳細については、[75 ページのセクション 12.3 「サイレントインストールの実行」](#) を参照してください。

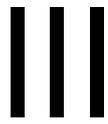
9.2 アプライアンスインストール

アプライアンスインストールは、SLES 11 SP3 64 ビットオペレーティングシステムと Sentinel の両方をインストールします。

Sentinel アプライアンスは、次のフォーマットで使用できます。

- ◆ OVF アプライアンスイメージ
- ◆ ハードウェアアプライアンス Live DVD イメージ (ハードウェアサーバに直接展開可能)

アプライアンスインストールの詳細については、[79 ページの第 13 章「アプライアンスインストール」](#)を参照してください。



Sentinel のインストール

このセクションでは、Sentinel および追加コンポーネントのインストールについて説明します。

- ◆ 65 ページの第 10 章「インストールの概要」
- ◆ 67 ページの第 11 章「インストールのチェックリスト」
- ◆ 69 ページの第 12 章「従来型インストール」
- ◆ 79 ページの第 13 章「アプライアンスインストール」
- ◆ 89 ページの第 14 章「NetFlow コレクタマネージャのインストール」
- ◆ 93 ページの第 15 章「コレクタとコネクタの追加インストール」
- ◆ 95 ページの第 16 章「インストールの検証」

10 インストールの概要

Sentinel をインストールすると、Sentinel サーバに次のコンポーネントがインストールされます。

- ◆ **Sentinel サーバプロセス** : Sentinel の主要コンポーネントです。Sentinel サーバプロセスは Sentinel の他のコンポーネントからの要求を処理し、システムのシームレスな機能を実現します。Sentinel サーバプロセスは、データのフィルタリング、検索クエリの処理、およびユーザー認証や権限付与などの管理タスクの管理といった要求を処理します。
- ◆ **Web サーバ** : Sentinel は、Sentinel の Web インタフェースに安全な接続ができるように、Web サーバに Jetty を採用しています。
- ◆ **PostgreSQL データベース** : Sentinel には組み込みデータベースが備わっており、Sentinel 設定情報、アセットおよび脆弱性データ、識別情報、インシデントおよびワークフローステータスなどはそこに格納されます。
- ◆ **MongoDB データベース** : セキュリティインテリジェンスデータを格納します。
- ◆ **コレクタマネージャ** : コレクタマネージャは、Sentinel に柔軟なデータ収集ポイントを提供します。Sentinel インストーラは、インストール時にデフォルトでコレクタマネージャをインストールします。
- ◆ **NetFlow コレクタマネージャ** : NetFlow コレクタマネージャはルータ、スイッチ、ファイアウォールなどのネットワークデバイスからネットワークフローデータ (NetFlow や IPFIX など) を収集します。ネットワークフローデータは、伝送されるパケットやバイトなどの、ホストの間のすべてのネットワーク接続に関する基本的な情報を示しています。これは、個々のホストまたはネットワーク全体の動作を視覚化するのに役立ちます。
- ◆ **相関エンジン** : 相関エンジンは、リアルタイムイベントストリームからのイベントを処理して、イベントが何らかの相関ルールをトリガするべきかどうかを判断します。
- ◆ **アドバイザ** : Security Nexus を搭載したアドバイザは、オプションのデータサブスクリプションサービスです。侵入検出と防止システムから、および企業脆弱性スキャン結果から、リアルタイムイベント間のデバイスレベルの相関関係を提供します。アドバイザの詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Detecting Vulnerabilities and Exploits](#)」を参照してください。
- ◆ **Sentinel のプラグイン** : Sentinel は、システムの機能を拡張および強化するさまざまなプラグインをサポートしています。これらのプラグインの一部はプリインストールされています。追加のプラグインおよびアップデートは、[Sentinel Plug-ins Web サイト](#)からダウンロードできます。Sentinel のプラグインには以下のものがあります。
 - ◆ コレクタ
 - ◆ コネクタ
 - ◆ 相関ルールとアクション
 - ◆ レポート
 - ◆ iTRAC ワークフロー
 - ◆ ソリューションパック

Sentinel のアーキテクチャは高度なスケーラビリティを備えており、高いイベント発生率が予想される場合は、コンポーネントを複数のマシンに分散し、そのシステムにとって最適なパフォーマンスを実現することができます。NetIQ 社では、運用環境では分散展開をセットアップすることを

推奨しています。そうすることにより、データ収集コンポーネントを別のマシンに分離することができ、これはシステムの安定性を最大限に保ちつつ、スパイクや他の異常に対処する上で重要です。詳細については、[39 ページのセクション 6.1「分散展開の利点」](#)を参照してください。

11 インストールのチェックリスト

インストールを開始する前に、次の作業を完了していることを確認してください。

- ハードウェアおよびソフトウェアが、[37 ページの第 5 章「システム要件を満たす」](#)に示されているシステム要件を満たしていることを確認します。
- 以前に Sentinel がインストールされていた環境の場合は、以前のインストール環境のファイルやシステム設定が残っていないことを確認します。詳細については、[177 ページの付録 B「アンインストール中」](#)を参照してください。
- ライセンス版のインストールを計画している場合は、[NetIQ Customer Care Center](#) からライセンスキーを取得してください。
- [55 ページの第 8 章「使用するポート」](#)に示されているポートがファイアウォールで開かれていることを確認します。
- Sentinel インストーラが正常に動作するためには、システムがホスト名や有効な IP アドレスを返すことができなければなりません。そのためには、`/etc/hosts` ファイル内の IP アドレスを含む行にホスト名を追加し、それから「`hostname -f`」と入力してホスト名が正しく表示されるようにします。
- Network Time Protocol (NTP) を使用して時刻を同期します。
- RHEL システムの場合**：パフォーマンスを最適化するには、PostgreSQL データベースに適したメモリ設定にする必要があります。SHMMAX パラメータは、1073741824 以上に設定する必要があります。

適切な値を設定するには、次の情報を `/etc/sysctl.conf` ファイルに追加してください。

```
# for Sentinel PostgreSQL
kernel.shmmax=1073741824
```

- 従来型インストールの場合**：

Sentinel サーバのオペレーティングシステムに、少なくとも SLES サーバか RHEL 6 サーバの Base Server コンポーネントが含まれている必要があります。Sentinel では、次の RPM の 64 ビットバージョンが必要です。

- ◆ bash
- ◆ bc
- ◆ coreutils
- ◆ gettext
- ◆ glibc
- ◆ grep
- ◆ libgcc
- ◆ libstdc
- ◆ lsof
- ◆ net-tools
- ◆ openssl
- ◆ python-libs

- ◆ sed
- ◆ zlib

12 従来型インストール

本章では、Sentinel をインストールするさまざまな方法について説明します。

- ◆ 69 ページのセクション 12.1 「インストールオプションについて」
- ◆ 70 ページのセクション 12.2 「インタラクティブインストールの実行」
- ◆ 75 ページのセクション 12.3 「サイレントインストールの実行」
- ◆ 76 ページのセクション 12.4 「非 root ユーザとして Sentinel をインストール」

12.1 インストールオプションについて

`./install-sentinel --help` は、次のオプションを示します。

オプション	値	説明
<code>--location</code>	ディレクトリ	Sentinel をインストールする、root (/) 以外のディレクトリを指定します。
<code>-m</code> 、 <code>--manifest</code>	ファイル名	デフォルトのマニフェストファイルの代わりに使用する製品マニフェストファイルを指定します。
<code>--no-configure</code>		インストール後に製品を設定しないことを指定します。
<code>-n</code> 、 <code>--no-start</code>		インストールまたは設定後に Sentinel を起動または再起動しないことを指定します。
<code>-r</code> 、 <code>--recordunattended</code>	ファイル名	無人インストールで使用するパラメータを記録するファイルを指定します。
<code>-u</code> 、 <code>--unattended</code>	ファイル名	指定されたファイルにあるパラメータを使用して、無人のシステム上に Sentinel をインストールします。
<code>-h</code> 、 <code>--help</code>		Sentinel のインストール中に使用できるオプションを表示します。
<code>-l</code> 、 <code>--log-file</code>	ファイル名	ログメッセージをファイルに記録します。
<code>--no-banner</code>		バナーメッセージの表示を抑制します。
<code>-q</code> 、 <code>--quiet</code>		メッセージ数を減らします。
<code>-v</code> 、 <code>--verbose</code>		インストール時にすべてのメッセージを表示します。

12.2 インタラクティブインストールの実行

本セクションでは、標準インストールおよびカスタムインストールについて説明します。

- ◆ 70 ページのセクション 12.2.1 「Sentinel サーバの標準インストール」
- ◆ 71 ページのセクション 12.2.2 「Sentinel サーバのカスタムインストール」
- ◆ 73 ページのセクション 12.2.3 「コレクタマネージャと関連エンジンのインストール」

12.2.1 Sentinel サーバの標準インストール

次の手順に従って、標準インストールを実行します。

- 1 [NetIQ ダウンロード Web サイト](#)から Sentinel インストールファイルをダウンロードします。
 - 1a **[製品または技術]** フィールドで **[SIEM-Sentinel]** をブラウズして選択します。
 - 1b **[検索]** をクリックします。
 - 1c **[Sentinel Evaluation]** の **[ダウンロード]** 列のボタンをクリックします。
 - 1d **[ダウンロードに進む]** をクリックし、お客様名とパスワードを入力します。
 - 1e お使いのプラットフォーム用のインストールバージョンに該当する **[ダウンロード]** をクリックします。
- 2 コマンドラインで次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

- 3 インストーラを抽出したディレクトリに移動します。

```
cd <directory_name>
```

- 4 次のコマンドを指定して、Sentinel をインストールします。

```
./install-sentinel
```

または

複数のシステムに Sentinel をインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを、他のシステムに対する Sentinel の無人インストールに使用できます。インストールオプションを記録するには、次のコマンドを指定します。

```
./install-sentinel -r <response_filename>
```

- 5 インストールに使用する言語の番号を指定してから、<Enter> を押します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。
- 6 スペースキーを押して使用許諾契約を確認します。
- 7 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。
- 8 選択を求められたら、「1」を指定して標準環境設定に進みます。

インストーラに付属のデフォルトの評価版ライセンスキーを使用してインストールを続行します。評価期間中または評価期間終了後の任意の時点で、評価版のライセンスを、購入したライセンスキーに置き換えることができます。

9 管理者ユーザ admin のパスワードを指定します。

10 パスワードを再度確認します。

このパスワードは、admin、dbauser、および appuser が使用します。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

12.2.2 Sentinel サーバのカスタムインストール

Sentinel をカスタム環境設定でインストールする場合、ライセンスキーを指定したり、ユーザごとにパスワードを変更したり、内部コンポーネントとのやり取りに使用されるポートごとに値を指定したりすることができます。

1 [NetIQ ダウンロード Web サイト](#) から Sentinel インストールファイルをダウンロードします。

1a **[製品または技術]** フィールドで **[SIEM-Sentinel]** をブラウズして選択します。

1b **[検索]** をクリックします。

1c **[Sentinel 7.2 Evaluation]** の **[ダウンロード]** 列のボタンをクリックします。

1d **[ダウンロードに進む]** をクリックし、お客様名とパスワードを入力します。

1e お使いのプラットフォーム用のインストールバージョンに該当する **[ダウンロード]** をクリックします。

2 コマンドラインで次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

3 抽出されたディレクトリのルートで次のコマンドを指定して、Sentinel をインストールします。

```
./install-sentinel
```

または

このカスタム環境設定を使用して複数のシステムに Sentinel をインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを、他のシステムに対する Sentinel の無人インストールに使用できます。インストールオプションを記録するには、次のコマンドを指定します。

```
./install-sentinel -r <response_filename>
```

4 インストールに使用する言語の番号を指定してから、<Enter> を押します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

5 スペースキーを押して使用許諾契約を確認します。

6 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。

- 7 Sentinel のカスタム環境設定を実行する場合は、「2」を指定します。
- 8 デフォルトの評価版ライセンスキーを使用するには、「1」を入力します。
または
購入した Sentinel ライセンスキーを入力するには、「2」を入力します。
- 9 管理者ユーザ admin のパスワードを指定し、パスワードを再度確認します。
- 10 データベースユーザ dbauser のパスワードを指定し、パスワードを再度確認します。
dbauser アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。
- 11 アプリケーションユーザ appuser のパスワードを指定し、パスワードを再度確認します。
- 12 目的の番号を入力してから新しいポート番号を指定して、Sentinel サービスのポート割り当てを変更します。
- 13 ポートを変更してから「7」を指定し、完了します。
- 14 内部データベースのみを使用してユーザを認証するには、「1」を入力します。
または
ドメインで LDAP ディレクトリを設定している場合に、LDAP ディレクトリ認証を使用してユーザを認証するには、「2」を入力します。
デフォルト値は 1 です。
- 15 **Sentinel を FIPS 140-2 モードにする場合は**、「y」を押します。
 - 15a キーストアデータベース用の強化パスワードを指定し、そのパスワードを再確認します。

注：パスワードは 7 文字以上にする必要があります。パスワードには、数字、ASCII 小文字、ASCII 大文字、ASCII 非英数字、および非 ASCII 文字の中から少なくとも 3 種類が含まれていなければなりません。
ASCII 大文字が最初の文字の場合、または数字が最後の文字の場合、それらは文字数にカウントされません。

 - 15b 外部証明書をキーストアデータベースに挿入してトラストを確立する場合は、「y」を押して証明書ファイルのパスを指定します。そうしない場合は、「n」を押します。
 - 15c [109 ページの第 21 章「FIPS 140-2 モードでの Sentinel の運用」](#)に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

`https://<IP_Address_Sentinel_server>:8443` .

`<IP_Address_Sentinel_server>` は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

12.2.3 コレクタマネージャと関連エンジンのインストール

デフォルトでは、Sentinel をインストールすると、コレクタマネージャと関連エンジンも 1 つずつインストールされます。NetIQ 社では、運用環境では分散展開をセットアップすることを推奨しています。そうすることにより、データ収集コンポーネントを別のマシンに分離することができ、これはシステムの安定性を最大限に保ちつつ、スパイクや他の異常に対処する上で重要です。追加コンポーネントのインストールの利点については、[39 ページのセクション 6.1「分散展開の利点」](#)を参照してください。

重要: 追加のコレクタマネージャまたは関連エンジンは別個のシステムにインストールする必要があります。コレクタマネージャまたは関連エンジンを、Sentinel サーバがインストールされている同じシステムにインストールすることはできません。

インストールのチェックリスト: インストールを開始する前に、次のタスクを完了していることを確認してください。

- ◆ ハードウェアとソフトウェアが最低要件を満たしていることを確認します。詳細については、[37 ページの第 5 章「システム要件を満たす」](#)を参照してください。
- ◆ Network Time Protocol (NTP) を使用して時刻を同期します。
- ◆ コレクタマネージャは、Sentinel サーバ上のメッセージバスポート (61616) にネットワーク接続する必要があります。コレクタマネージャのインストールを開始する前に、すべてのファイアウォールおよびネットワーク設定で、このポートでの通信が許可されていることを確認します。

コレクタマネージャと関連エンジンをインストールするには、次の手順を実行します。

- 1 Web ブラウザに次の URL を入力して、Sentinel Web インタフェースを起動します。

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

Sentinel サーバのインストール時に指定したユーザ名およびパスワードでログインします。

- 2 ツールバーで [ダウンロード] をクリックします。
- 3 必要なインストールで [インストーラのダウンロード] をクリックします。
- 4 [ファイルの保存] をクリックして、目的の場所にインストーラを保存します。
- 5 次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

- 6 インストーラを抽出したディレクトリに移動します。
- 7 次のコマンドを指定して、コレクタマネージャまたは関連エンジンをインストールします。

コレクタマネージャの場合:

```
./install-cm
```

関連エンジンの場合:

```
./install-ce
```

または

複数のシステムにコレクタマネージャまたは関連エンジンをインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを、他のシステムに対するの無人インストールに使用できます。インストールオプションを記録するには、次のコマンドを指定します。

コレクタマネージャの場合：

```
./install-cm -r <response_filename>
```

関連エンジンの場合：

```
./install-ce -r <response_filename>
```

- 8 インストールに使用する言語の番号を指定します。
エンドユーザの使用許諾契約が、選択した言語で表示されます。
- 9 スペースキーを押して使用許諾契約を確認します。
- 10 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。
インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。
- 11 プロンプトが表示されたら、適切なオプションを指定して、標準またはカスタムの環境設定を進めます。
- 12 デフォルトの Communication Server ホスト名または、Sentinel がインストールされているマシンの IP アドレスを入力します。
- 13 (条件による) カスタム環境設定を選択した場合は、次の項目を指定します。
 - 13a Sentinel サーバ通信チャンネルのポート番号。
 - 13b Sentinel Web サーバのポート番号。
- 14 証明書の受諾を求めるプロンプトが表示されたら、Sentinel サーバで次のコマンドを実行して、証明書を検証します。

FIPS モードの場合：

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore  
/etc/opt/novell/sentinel/config/.activemqkeystore.jks
```

非 FIPS モードの場合：

```
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore  
/etc/opt/novell/sentinel/config/nonfips_backup/.activemqkeystore.jks
```

証明書の出力を [ステップ 12](#) で表示された Sentinel サーバ証明書と比較します。

注：証明書が一致しない場合は、インストールが停止します。インストールのセットアップを再実行して、証明書を確認してください。

- 15 証明書の出力が Sentinel サーバ証明書と一致しているなら、その証明書を受諾します。
- 16 admin パスワードを指定します。
- 17 (条件による) カスタム環境設定を選択する場合は、「yes」または「y」と入力し、Sentinel で FIPS 140-2 モードを有効にして、FIPS 環境設定を続行します。
- 18 インストールが完了するまで、プロンプトの指示に従ってインストールを続行します。

12.3 サイレントインストールの実行

複数の Sentinel サーバ、コレクタマネージャまたは関連エンジンをインストールして展開する必要がある場合は、サイレントインストール(無人インストール)が便利です。そのような場合には、インタラクティブインストール中にインストールパラメータを記録し、記録したファイルをその他のサーバで実行します。

サイレントインストールを実行する場合、インストールパラメータをファイルに記録してあることを確認してください。レスポンスファイルの作成については、[70 ページのセクション 12.2.1 「Sentinel サーバの標準インストール」](#) または [71 ページのセクション 12.2.2 「Sentinel サーバのカスタムインストール」](#) および [73 ページのセクション 12.2.3 「コレクタマネージャと関連エンジンのインストール」](#) を参照してください。

FIPS 140-2 モードを有効にする場合は、次のパラメータがレスポンスファイルに含まれていることを確認します。

- ◆ ENABLE_FIPS_MODE
- ◆ NSS_DB_PASSWORD

サイレントインストールを実行するには、以下のステップを行います。

- 1 [NetIQ ダウンロード Web サイト](#) からインストールファイルをダウンロードします。
- 2 Sentinel、コレクタマネージャまたは関連エンジンをインストールするサーバに、root としてログインします。
- 3 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

```
tar -zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

- 4 次のコマンドを指定して、サイレントモードでインストールを実行します。

Sentinel サーバの場合：

```
./install-sentinel -u <response_file>
```

コレクタマネージャの場合：

```
./install-cm -u <response_file>
```

関連エンジンの場合：

```
./install-ce -u <response_file>
```

インストールは、レスポンスファイルに格納された値を使用して進行します。

Sentinel サーバをインストールした場合は、インストール後にすべてのサービスが開始されるまでに数分かかることがあります。これは、システムが 1 回限りの初期化を実行するためです。インストールが完了してから、サーバにログインしてください。

- 5 (条件による) Sentinel サーバの **FIPS 140-2 モードを有効にする場合は、[109 ページの第 21 章 「FIPS 140-2 モードでの Sentinel の運用」](#) に示されているタスクを行って、FIPS 140-2 モード設定を完了します。**

12.4 非 root ユーザとして Sentinel をインストール

組織のポリシーにより、root として Sentinel を完全インストールすることを許可されていない場合は、Sentinel を非 root ユーザ、つまり novell ユーザとしてインストールすることができます。この方法でインストールする場合、root ユーザとしていくつかのステップを実行した後、root ユーザによって作成された novell ユーザとして Sentinel をインストールします。最後に、root ユーザとしてインストールを完了します。

非 root ユーザとして Sentinel をインストールする場合は、novell ユーザとして Sentinel をインストールする必要があります。NetIQ 社では、novell ユーザ以外の非 root ユーザのインストール環境はサポートしていませんが、その場合でもインストールは正常に完了します。

注：デフォルト以外の既存のディレクトリに Sentinel をインストールする場合は、そのディレクトリに対する所有権を novell ユーザが所持していることを確認してください。次のコマンドを実行して、所有権を割り当てます。

```
chown novell:novell <non-default installation directory>
```

- 1 [NetIQ ダウンロード Web サイト](#) からインストールファイルをダウンロードします。
- 2 コマンドラインで次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

```
tar -zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

- 3 root として Sentinel をインストールするサーバに root としてログインします。
- 4 次のコマンドを指定します。

```
./bin/root_install_prepare
```

root 権限で実行するコマンドの一覧が表示されます。非 root ユーザにデフォルト以外の場所に Sentinel をインストールさせたい場合は、コマンドに加えて --location オプションも指定します。例：

```
./bin/root_install_prepare --location=/foo
```

--location オプションに渡す値 foo は、ディレクトリパスの前に付加されます。

これによって、novell グループおよび novell ユーザが存在しなければ、それらが作成されます。

- 5 コマンドリストを受け入れます。
表示されたコマンドが実行されます。
- 6 次のコマンドを指定して、新しく作成された非 root ユーザ (つまり novell) に変更します。

```
su novell
```

- 7 (条件による) インタラクティブインストールを実行するには：

7a インストールしているコンポーネントに応じて適切なコマンドを指定します。

コンポーネント	コマンド
Sentinel サーバ	デフォルトの場所 : <code>./install-sentinel</code>
	デフォルト以外の場所 : <code>./install-sentinel --location=/foo</code>
コレクタマネージャ	デフォルトの場所 : <code>./install-cm</code>
	デフォルト以外の場所 : <code>./install-cm --location=/foo</code>
関連エンジン	デフォルトの場所 : <code>./install-ce</code>
	デフォルト以外の場所 : <code>./install-cm --location=/foo</code>
NetFlow コレクタマネージャ	デフォルトの場所 : <code>./install-netflow</code>
	デフォルト以外の場所 : <code>./install-netflow --location=/foo</code>

7b ステップ 9に進みます。

- 8** (条件による) サイレントインストールを実行する場合、インストールパラメータをファイルに記録してあることを確認してください。レスポンスファイルの作成については、[70 ページのセクション 12.2.1 「Sentinel サーバの標準インストール」](#) または [71 ページのセクション 12.2.2 「Sentinel サーバのカスタムインストール」](#) を参照してください。

サイレントインストールを実行するには：

- 8a** インストールしているコンポーネントに応じて適切なコマンドを指定します。

コンポーネント	コマンド
Sentinel サーバ	デフォルトの場所 : <code>./install-sentinel -u <response_file></code>
	デフォルト以外の場所 : <code>./install-sentinel --location=/foo -u <response_file></code>
コレクタマネージャ	デフォルトの場所 : <code>./install-cm -u <response_file></code>
	デフォルト以外の場所 : <code>./install-cm --location=/foo -u <response_file></code>
関連エンジン	デフォルトの場所 : <code>./install-ce -u <response_file></code>
	デフォルト以外の場所 : <code>./install-ce --location=/foo -u <response_file></code>
NetFlow コレクタマネージャ	デフォルトの場所 : <code>./install-netflow -u <response_file></code>
	デフォルト以外の場所 : <code>./install-netflow --location=/foo -u <response_file></code>

インストールは、レスポンスファイルに格納された値を使用して進行します。

8b ステップ 12に進みます。

- 9** インストールに使用する言語の番号を指定します。
 エンドユーザの使用許諾契約が、選択した言語で表示されます。
- 10** エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。
 すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

11 インストールのモードを指定するように求められます。

- ◆ 標準環境設定で続行する場合は、70 ページのセクション 12.2.1 「Sentinel サーバの標準インストール」のステップ 8 からステップ 10 に従って手順を進めます。
- ◆ カスタム環境設定で続行する場合は、71 ページのセクション 12.2.2 「Sentinel サーバのカスタムインストール」のステップ 7 からステップ 14 に従って手順を進めます。

12 root ユーザとしてログインし、次のコマンドを指定してインストールを完了します。

```
./bin/root_install_finish
```

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

Sentinel Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

13 アプライアンスインストール

Sentinel アプライアンスは SUSE Studio で構築された、すぐに実行可能なソフトウェアアプライアンスです。このアプライアンスは、強化された SLES オペレーティングシステムと Sentinel ソフトウェア統合アップデートサービスを組み合わせて、お客様が既存の投資を活用できるように、簡単にシームレスなユーザエクスペリエンスを提供します。Sentinel アプライアンスをインストールする前に、サポートされている SLES [リリースノート](#) で新しい機能と既知の問題を確認してください。

Sentinel のアプライアンスイメージが、ISO 形式と仮想環境にデプロイできる OVF 形式の両方でパッケージされています。サポートされる仮想化プラットフォームについては、[NetIQ Sentinel の技術情報 Web サイト](#) を参照してください。

- ◆ [79 ページのセクション 13.1 「Sentinel ISO アプライアンスのインストール」](#)
- ◆ [82 ページのセクション 13.2 「Sentinel OVF アプライアンスのインストール」](#)
- ◆ [84 ページのセクション 13.3 「アプライアンスのインストール後の環境設定」](#)
- ◆ [87 ページのセクション 13.4 「WebYaST を使用したサーバの起動と停止」](#)

13.1 Sentinel ISO アプライアンスのインストール

このセクションでは、ISO アプライアンスイメージを使用して Sentinel、コレクタマネージャ、および関連エンジンをインストールする方法について説明します。このイメージ形式では、ブート可能な ISO DVD イメージを使って物理 (ベアメタル) または仮想 (ハイパーバイザでアンインストールされた仮想マシン) のハードウェアに直接デプロイできる、完全なディスクイメージ形式を生成できます。

- ◆ [79 ページのセクション 13.1.1 「前提条件」](#)
- ◆ [80 ページのセクション 13.1.2 「Sentinel のインストール」](#)
- ◆ [81 ページのセクション 13.1.3 「コレクタマネージャと関連エンジンのインストール」](#)

13.1.1 前提条件

Sentinel を ISO アプライアンスとしてインストールする環境が、以下の前提条件を満たしていることを確認します。

- ◆ (条件付き) Sentinel ISO アプライアンスをベアメタルハードウェアにインストールする場合、アプライアンス ISO のディスクイメージをサポートサイトからダウンロードし、ファイルを解凍して DVD を作成します。
- ◆ ISO ディスクイメージをインストールするシステムに、インストールの完了に必要な 4.5GB 以上のメモリが搭載されていることを確認します。
- ◆ インストーラが自動パーティション提案を作成するのに必要な 50GB 以上のハードディスク容量が存在することを確認します。

13.1.2 Sentinel のインストール

Sentinel ISO アプライアンスをインストールするには、次のようにします。

- 1 ISO 仮想アプライアンスイメージを [NetIQ ダウンロード Web サイト](#) からダウンロードします。
- 2 (条件付き) ハイパーバイザを使用している場合は、次のようにします。

ISO 仮想アプライアンスイメージを使用する仮想マシンをセットアップし、起動します。

または

ISO イメージを DVD にコピーし、DVD を使用して仮想マシンをセットアップし、起動します。

- 3 (条件付き) Sentinel アプライアンスをベアメタルハードウェアにインストールする場合は、次のようにします。

3a DVD ドライブからその DVD を使用して物理マシンをブートします。

3b インストールウィザードの画面上の指示に従います。

3c ブートメニューの一番上のエントリを選択して、ライブ DVD のアプライアンスイメージを実行します。

最初に使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは自動的に終了します。使用可能なメモリが 2.5GB 以上 6.7GB 未満の場合、推奨よりもメモリの容量が少ないというメッセージが表示されます。インストールを続行する場合は「y」と入力し、続行しない場合は「n」と入力します。

- 4 使用する言語を選択して、[次へ] をクリックします。
- 5 キーボードの環境設定を選択して、[次へ] をクリックします。
- 6 SUSE Enterprise Server ソフトウェア使用許諾契約書の条項を確認して同意します。[次へ] をクリックします。
- 7 NetIQ Sentinel の使用許諾契約の条項を確認して同意します。[次へ] をクリックします。
- 8 [ホスト名] および [ドメイン名] 画面で、ホスト名とドメイン名を指定します。[ホスト名をループバック IP に割り当てる] の選択を解除します。
- 9 [次へ] をクリックします。
- 10 次の接続設定のいずれかを選択します。
 - ◆ 現在のネットワーク接続設定を使用するには、[ネットワーク環境設定 II] ページで [次の環境設定を使用する] を選択します。
 - ◆ ネットワーク接続設定を変更するには、[変更] をクリックし、目的の変更を行います。
- 11 [Next(次へ)] をクリックします。
- 12 日付と時刻を設定して、[次へ] をクリックします。

インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻の設定を変更することはできません。インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

```
rcntp restart
```
- 13 root のパスワードを設定して、[次へ] をクリックします。

- 14 Sentinel 管理者のパスワードを設定して、[次へ] をクリックします。

物理サーバにアプライアンスをインストールする場合、[**Sentinel アプライアンスをハードドライブにインストールします (ライブ DVD イメージ専用)**] が選択されていることを確認してください。デフォルトではこのオプションが選択されています。

このチェックボックスのチェックを外すと、アプライアンスは物理サーバにインストールされず、ライブ DVD モードのみで実行されます。[ステップ 21](#)に進みます。
- 15 YaST2 ライブインストーラのコンソールで、[次へ] を選択します。

YaST2 ライブインストーラのコンソールにより、アプライアンスがハードディスクにインストールされます。YaST2 ライブインストーラのコンソールは、インストールの前半のステップの一部を繰り返します。
- 16 [推奨されるパーティション化] 画面に、推奨されるパーティションのセットアップが表示されます。パーティションのセットアップを確認し、(必要な場合) セットアップを設定してから、[次へ] を選択します。これらの設定の変更は、SLES でのパーティションの環境設定に習熟している場合にのみ行ってください。

画面上のさまざまなパーティション化オプションを使用して、パーティションのセットアップを設定できます。パーティションの環境設定について詳しくは、*SLES のマニュアル*にある「[Using the YaST Partitioner](#)」および [45 ページのセクション 6.6 「データストレージのパーティション計画」](#)を参照してください。
- 17 ルートパスワードを入力し、[次へ] を選択します。
- 18 [ライブインストール設定] 画面に、選択したインストール設定が表示されます。設定を確認し、(必要な場合は) 設定を環境設定してから、[インストール] を選択します。
- 19 [インストール] を選択して、インストールの確認を行います。

インストールが完了するまで待機します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。
- 20 [OK] を選択して、システムを再起動します。
- 21 コンソールに表示されたアプライアンスの IP アドレスをメモします。
- 22 コンソールでルートユーザ名とパスワードを入力して、アプライアンスにログインします。

ユーザ名のデフォルト値は root で、パスワードは[ステップ 17](#) で設定したものです。
- 23 [84 ページのセクション 13.3 「アプライアンスのインストール後の環境設定」](#)に従って手順を進めます。

13.1.3 コレクタマネージャと関連エンジンのインストール

コレクタマネージャや関連エンジンのインストール手順もほぼ同じですが、[NetIQ ダウンロード Web サイト](#)から該当する ISO アプライアンスファイルをダウンロードする必要があります。

- 1 [80 ページのセクション 13.1.2 「Sentinel のインストール」](#)の手順 1 から[ステップ 13](#) を完了させます。
- 2 コレクタマネージャまたは関連エンジンのために、次の環境設定を指定します。
 - ◆ **Sentinel サーバのホスト名または IP アドレス** : コレクタマネージャまたは関連エンジンが接続する Sentinel サーバのホスト名または IP アドレスを指定します。
 - ◆ **Sentinel 通信チャンネルポート** : Sentinel サーバ通信チャンネルポートの番号を指定します。デフォルトのポート番号は 61616 です。
 - ◆ **Sentinel Web サーバポート** : Sentinel Web サーバポートを指定します。デフォルトポートは 8443 です。

- ◆ **Sentinel サーバの admin ユーザパスワード** : admin ユーザのパスワードを指定します。
- ◆ **Sentinel アプライアンスをハードドライブにインストールします (ライブ DVD イメージ専用)** : 物理サーバへアプライアンスをインストールする場合、このチェックボックスが選択されていることを確認してください。

このチェックボックスの選択を解除すると、アプライアンスは物理サーバにインストールされず、LIVE DVD モードでのみ実行されます。

- 3 [次へ] をクリックします。
- 4 同意を求められたら、証明書に同意します。
- 5 [80 ページのセクション 13.1.2 「Sentinel のインストール」](#) のステップ 15 からステップ 20 を実行します。
- 6 コンソールに表示されたアプライアンスの IP アドレスをメモします。
何をインストールしたかに応じて、このアプライアンスが Sentinel コレクタマネージャまたは
相関エンジンであることを示すメッセージとその IP アドレスがコンソールに表示されます。
コンソールには、Sentinel サーバのユーザインタフェース IP アドレスも表示されます。
- 7 [80 ページのセクション 13.1.2 「Sentinel のインストール」](#) のステップ 22 からステップ 23 を実行します。

13.2 Sentinel OVF アプライアンスのインストール

このセクションでは、Sentinel、コレクタマネージャ、および相関エンジンを、OVF アプライアンスイメージとしてインストールする場合について説明します。

OVF フォーマットは、ほとんどのハイパーバイザで、直接または単純変換によってサポートされている標準の仮想マシンフォーマットです。Sentinel は、OVF アプライアンスを 2 つの認定ハイパーバイザでサポートしていますが、それ以外のハイパーバイザでも使用できます。

- ◆ [82 ページのセクション 13.2.1 「Sentinel のインストール」](#)
- ◆ [83 ページのセクション 13.2.2 「コレクタマネージャと相関エンジンのインストール」](#)

13.2.1 Sentinel のインストール

Sentinel OVF アプライアンスをインストールするには、次のようにします。

- 1 OVF 仮想アプライアンスイメージを [NetIQ ダウンロード Web サイト](#) からダウンロードします。
- 2 ハイパーバイザの管理コンソールで、OVF イメージファイルを新規仮想マシンとしてインポートします。OVF イメージをネイティブフォーマットに変換するように要求された場合に、ハイパーバイザが変換できるようにします。
- 3 新規仮想マシンに割り当てられた仮想ハードウェアリソースが、Sentinel の要件を満たしているか確認します。
- 4 仮想マシンの電源をオンにします。
- 5 使用する言語を選択して、[次へ] をクリックします。
- 6 キーボードのレイアウトを選択して、[次へ] をクリックします。
- 7 SUSE Linux Enterprise Server (SLES) 11 SP3 ソフトウェア使用許諾契約書の条項を確認して同意します。
- 8 NetIQ Sentinel の使用許諾契約の条項を確認して同意します。

- 9 [ホスト名] および [ドメイン名] 画面で、ホスト名とドメイン名を指定します。[ホスト名をループバック IP に割り当てる] の選択を解除します。
- 10 [Next] をクリックします。ホスト名の環境設定が保存されます。
- 11 次のネットワーク接続オプションのいずれかを選択します。
 - ◆ 現在のネットワーク接続設定を使用するには、[ネットワーク環境設定 II] ページで [次の環境設定を使用する] を選択して、[次へ] をクリックします。
 - ◆ ネットワーク接続設定を変更するには、[変更] を選択して目的の変更を行ってから、[次へ] をクリックします。ネットワーク接続設定が保存されます。
- 12 日付と時刻を設定して、[次へ] をクリックします。

インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできませんが、NTP の環境設定を変更することはできません。

インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

```
rcntp restart
```
- 13 root のパスワードを設定して、[Next] をクリックします。

使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは続行できません。[次へ] ボタンはグレー表示となり、使用できません。

使用可能なメモリが 2.5GB 以上 6.7GB 未満の場合、推奨よりもメモリの容量が少ないというメッセージが表示されます。このメッセージが表示されたら、[Next] をクリックしてインストールを続行します。
- 14 Sentinel 管理者のパスワードを設定して、[次へ] をクリックします。

システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。
- 15 コンソールに表示されたアプライアンスの IP アドレスをメモします。Sentinel Web コンソールにアクセスする IP アドレスと同じものを使用します。

13.2.2 コレクタマネージャと関連エンジンのインストール

コレクタマネージャまたは関連エンジンを VMware ESX サーバに OVF アプライアンスイメージとしてインストールするには：

- 1 82 ページのセクション 13.2.1 「Sentinel のインストール」 の手順 1 から 10 を実行します。
- 2 コレクタマネージャが接続する Sentinel サーバのホスト名または IP アドレスを指定します。
- 3 Communication Server のポート番号を指定します。デフォルトポートは 61616 です。
- 4 admin パスワードを指定します。
- 5 次へをクリックします。
- 6 証明書を受け入れます。

7 [次へ] をクリックしてインストールを完了します。

インストールが完了すると、どちらをインストールしたかに応じて、インストーラはこのアプライアンスが Sentinel コレクタマネージャまたは Sentinel 関連エンジンであることを示すメッセージと、その IP アドレスを表示します。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

13.3 アプライアンスのインストール後の環境設定

Sentinel をインストールした後、アプライアンスが正常に動作するように環境設定をさらに行う必要があります。

- ◆ 84 ページのセクション 13.3.1 「WebYaST の環境設定」
- ◆ 84 ページのセクション 13.3.2 「パーティションの作成」
- ◆ 85 ページのセクション 13.3.3 「アップデートの登録」
- ◆ 86 ページのセクション 13.3.4 「SMT でのアプライアンスの設定」
- ◆ 87 ページのセクション 13.3.5 「VMware Tools のインストール (VMware ESX サーバにのみ適用)」

13.3.1 WebYaST の環境設定

Sentinel アプライアンスのユーザインタフェースには WebYaST が備わっています。WebYaST とは、アプライアンスを制御するための Web ベースのリモートコンソールで、SUSE Linux Enterprise をベースにしています。WebYaST を使用して、Sentinel アプライアンスに対するアクセス、環境設定、監視を行います。次に、WebYaST の環境設定の手順について簡単に説明します。環境設定の詳細については、『[WebYaST User Guide \(http://www.novell.com/documentation/webyast/\)](http://www.novell.com/documentation/webyast/)』を参照してください。

- 1 Sentinel アプライアンスにログインします。
- 2 [アプライアンス] をクリックします。
- 3 85 ページのセクション 13.3.3 「アップデートの登録」の説明にあるように、アップデートを受信する Sentinel サーバの環境設定を行います。
- 4 [次へ] をクリックして、初期設定を完了します。

13.3.2 パーティションの作成

ベストプラクティスとして、別個のパーティションを作成して、実行可能ファイル、環境設定ファイル、オペレーティングシステムファイルとは別のパーティションに Sentinel データを保存できるようにしてください。可変データを別に保存することには、一連のファイルのバックアップが容易になり、破損した場合の回復が簡単になるというメリットがあるうえ、ディスクパーティションが満杯になった場合の堅牢性が向上します。パーティションの計画については、[45 ページのセクション](#)

ン 6.6 「[データストレージのパーティション計画](#)」を参照してください。YaST ツールを使用して、アプライアンスにパーティションを追加し、新しいパーティションにディレクトリを移動させることができます。

次の手順で新しいパーティションを作成し、データファイルを元のディレクトリから新しく作成したパーティションに移動させます。

1 Sentinel に root としてログインします。

2 次のコマンドを実行して、アプライアンス上の Sentinel を停止させます。

```
/etc/init.d/sentinel stop
```

3 次のコマンドを指定して、novell ユーザに変更します。

```
su -novell
```

4 /var/opt/novell/sentinel のディレクトリの内容を一時的にどこかの場所に移動します。

5 root ユーザに変更します。

6 次のコマンドを入力して、YaST2 コントロールセンターにアクセスします。

```
yast
```

7 [システム] > [パーティショナ] の順に選択します。

8 警告を確認して [はい] を選択し、新しい未使用パーティションを追加します。

パーティションの作成について詳しくは、*SLES 11* のマニュアルにある「[Using the YaST Partitioner](#)」を参照してください。

9 /var/opt/novell/sentinel に新しいパーティションをマウントします。

10 次のコマンドを指定して、novell ユーザに変更します。

```
su -novell
```

11 ディレクトリの内容を一時保存先 ([ステップ 4](#) で保存した場所) から、新しいパーティション内の /var/opt/novell/sentinel に戻します。

12 次のコマンドを実行して、Sentinel アプライアンスを再起動します。

```
/etc/init.d/sentinel start
```

13.3.3 アップデートの登録

Sentinel アプライアンスをアプライアンス更新チャンネルに登録して、パッチの更新を受信できるようにする必要があります。アプライアンスを登録するには、まずアプライアンス登録コードまたはアプライアンスアクティベーションキーを [NetIQ Customer Care Center](#) から取得する必要があります。

以下の手順を行って、更新できるようにアプライアンスを登録します。

1 Sentinel アプライアンスにログインします。

2 [アプライアンス] をクリックして、WebYaST を起動します。

3 [登録] をクリックします。

4 アップデートを受信する電子メール ID を指定してから、システム名およびアプライアンス登録コードを指定します。

5 [保存] をクリックします。

13.3.4 SMT でのアプライアンスの設定

インターネットに直接アクセスできない保護された環境でアプライアンスを実行する必要がある場合は、Subscription Management Tool (SMT) でアプライアンスを設定できます。これにより、Sentinel の最新バージョンが公開されると、アプライアンスを最新バージョンにアップグレードできます。SMT は、NetIQ Customer Center に統合されたパッケージ代理システムで、主な NetIQ Customer Center 機能を提供します。

- ◆ [86 ページの「前提条件」](#)
- ◆ [87 ページの「アプライアンスの設定」](#)
- ◆ [87 ページの「アプライアンスのアップグレード」](#)

前提条件

- ◆ 更新する Sentinel 用の NetIQ Customer Center 資格情報を NetIQ から入手します。資格情報の入手方法については、[NetIQ サポート](#)にお問い合わせください。
- ◆ SMT をインストールするマシンに次のパッケージと共に SLES 11 SP3 がインストールされていることを確認します。
 - ◆ `htmldoc`
 - ◆ `perl-DBIx-Transaction`
 - ◆ `perl-File-Basename-Object`
 - ◆ `perl-DBIx-Migration-Director`
 - ◆ `perl-MIME-Lite`
 - ◆ `perl-Text-ASCIITable`
 - ◆ `yum-metadata-parser`
 - ◆ `createrepo`
 - ◆ `perl-DBI`
 - ◆ `apache2-prefork`
 - ◆ `libapr1`
 - ◆ `perl-Data-ShowTable`
 - ◆ `perl-Net-Daemon`
 - ◆ `perl-Tie-IxHash`
 - ◆ `fltk`
 - ◆ `libapr-util1`
 - ◆ `perl-PIRPC`
 - ◆ `apache2-mod_perl`
 - ◆ `apache2-utils`
 - ◆ `apache2`
 - ◆ `perl-DBD-mysql`
- ◆ SMT をインストールし、SMT サーバを設定します。詳細については、[SMT のマニュアル](#)の以下に関するセクションを参照してください。
 - ◆ [SMT のインストール](#)

- ◆ SMT サーバの設定
- ◆ SMT でのインストールと更新リポジトリのミラーリング
- ◆ アプライアンスコンピュータに wget ユーティリティをインストールします。

アプライアンスの設定

SMT を使用したアプライアンスの環境設定については、『[Subscription Management Tool \(SMT\) for SUSE Linux Enterprise 11](#)』マニュアルを参照してください。

アプライアンスリポジトリを有効にするには、次のコマンドを実行します。

```
smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64
```

```
smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64
```

```
smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
```

アプライアンスのアップグレード

アプライアンスのアップグレードについては、[136 ページのセクション 25.3 「SMT を使用したアプライアンスのアップグレード」](#)を参照してください。

13.3.5 VMware Tools のインストール (VMware ESX サーバにのみ適用)

Sentinel を VMware ESX サーバ上で効率的に動作させるには、VMware Tools をインストールする必要があります。VMware Tools は、仮想マシンのオペレーティングシステムのパフォーマンスを向上させるユーティリティスイートです。仮想マシンの管理も改善されます。VMware Tools のインストールの詳細については、『[VMware Tools for Linux Guests](#)』を参照してください。

VMware のマニュアルについては、『[Workstation User's Manual](#)』を参照してください。

13.4 WebYaST を使用したサーバの起動と停止

次のように Web インタフェースを使用して、Sentinel サーバを起動および停止できます。

- 1 Sentinel アプライアンスにログインします。
- 2 [アプライアンス] をクリックして、WebYaST を起動します。
- 3 [システムサービス] をクリックします。
- 4 Sentinel サーバを停止するには、[停止] をクリックします。
- 5 Sentinel サーバを起動するには、[開始] をクリックします。

14 NetFlow コレクタマネージャのインストール

NetFlow コレクタマネージャは、Sentinel サーバ、コレクタマネージャ、または関連エンジンがインストールされているのと同じコンピュータではなく、別個のコンピュータにインストールする必要があります。

14.1 インストールのチェックリスト

インストールを開始する前に、次のタスクを完了していることを確認してください。

- ハードウェアとソフトウェアが最低要件を満たしていることを確認します。詳細については、[37 ページの第 5 章「システム要件を満たす」](#)を参照してください。
- Network Time Protocol (NTP) を使用して時刻を同期します。

14.2 NetFlow コレクタマネージャのインストール

以下のいずれかの方法を使用して、NetFlow コレクタマネージャをインストールできます。

- ◆ **標準** : NetFlow 環境設定にデフォルト値を使用します。
- ◆ **カスタム** : Sentinel サーバのポート番号をカスタマイズできます。

注

- ◆ ネットワークフローデータを Sentinel サーバに送信するには、管理者であるか、NetFlow プロバイダの役割に属しているか、または NetFlow データの送信に関する許可を持っている必要があります。
- ◆ 複数の NetFlow コレクタマネージャのインストールを計画している場合、NetFlow コレクタマネージャごとに新しいユーザアカウントを作成して、NetFlow コレクタマネージャがネットワークフローデータを Sentinel に送信できるようにする必要があります。NetFlow コレクタマネージャごとに別々のユーザアカウントを持つようにすると、どの NetFlow コレクタマネージャが Sentinel にデータを送信できるかに関して追加レベルの制御が行えるようになります。

NetFlow コレクタマネージャをインストールするには、以下を行います。

- 1 Web インタフェースに次の URL を入力して、Sentinel Web インタフェースを起動します。

```
https://<IP_Address_Sentinel_server>:8443
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

Sentinel サーバのインストール中に指定したユーザ名とパスワードでログインします。

- 2 ツールバーで **[ダウンロード]** をクリックします。

- 3 NetFlow コレクタマネージャの見出しの下にある [インストーラのダウンロード] をクリックします。
- 4 [ファイルの保存] をクリックして、目的の場所にインストーラを保存します。
- 5 コマンドプロンプトで、以下のコマンドを指定してインストールファイルを抽出します。

```
tar zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

- 6 インストーラを抽出したディレクトリに移動します。

```
cd <directory_name>
```

- 7 次のコマンドを指定して、NetFlow コレクタマネージャをインストールします。

```
./install-netflow
```

- 8 インストールに使用する言語の番号を指定してから、<Enter> を押します。
- 9 スペースキーを押して使用許諾契約を確認します。
- 10 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。
インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。
- 11 標準かカスタムのどちらのインストールに進むかを指定します。
- 12 ネットワークフローデータを受け取る Sentinel サーバのホスト名または IP アドレスを指定します。
- 13 (条件による) カスタムインストールを選択した場合、Sentinel サーバのポート番号を指定します。
デフォルトのポート番号は 8443 です。
- 14 Sentinel サーバの認証を行うために、ユーザー名とパスワードを指定します。

注：指定したユーザ資格情報に、NetFlow データの送信に関する許可または管理特権が含まれているか確認します。それらが含まれていない場合、インストールは完了するものの、NetFlow コレクタマネージャがデータを Sentinel サーバに送信したときに認証が失敗します。

インストールが完了します。NetFlow コレクタマネージャが Sentinel サーバへの接続を確立するのに数分かかる場合があります。

- 15 (条件による) 以下のいずれかを実行して、NetFlow コレクタマネージャのインストールが成功したかどうかを判別できます。
 - ◆ NetFlow コレクタマネージャサービスが実行されているかどうかを検証します。

```
/etc/init.d/sentinel status
```
 - ◆ NetFlow コレクタマネージャが Sentinel サーバとの接続を確立しているかどうかを検証します。

```
netstat -an |grep 'ESTABLISHED' |grep <HTTPS_port_number>
```
 - ◆ [コレクション] > [NetFlow] をクリックして、NetFlow コレクタマネージャが Sentinel Web コンソールに表示されるかどうかを検証します。

- 16** ネットワークフローデータの収集元のデバイスでのネットワークフロートラフィックの転送を有効にします。

デバイスでの NetFlow の有効化の一部として、Sentinel サーバの IP アドレスと、NetFlow が有効にされたデバイスからのデータを NetFlow コレクタマネージャが受け取るポートの IP アドレスを指定する必要があります。デフォルトポート番号は 3578 です。詳細については、特定の NetFlow が有効にされたデバイスのマニュアルを参照してください。

15 コレクタとコネクタの追加インストール

デフォルトでは、Sentinel をインストールすると、リリースされているすべてのコレクタおよびコネクタがインストールされます。Sentinel のリリース以後にリリースされた新しいコレクタまたはコネクタをインストールする場合は、以下のセクションにある情報を参考にしてください。

- ◆ 93 ページのセクション 15.1 「コレクタのインストール」
- ◆ 93 ページのセクション 15.2 「コネクタのインストール」

15.1 コレクタのインストール

次の手順に従って、コレクタをインストールします。

- 1 Sentinel プラグインの Web ページから、希望するコレクタをダウンロードします。
- 2 `https://<IP address>:8443` で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。
- 3 ツールバーで [アプリケーション] をクリックしてから、[アプリケーション] をクリックします。
- 4 [コントロールセンターの起動] をクリックして Sentinel コントロールセンターを起動します。
- 5 ツールバーで、[イベントソースの管理] > [ライブビュー] の順にクリックし、[ツール] > [プラグインのインポート] の順にクリックします。
- 6 ステップ 1 でダウンロードしたコレクタファイルをブラウザして選択してから、[次へ] をクリックします。
- 7 残りのプロンプトに従った後、[終了] をクリックします。

コレクタを環境設定するには、Sentinel プラグイン Web サイトにある、特定のコレクタのマニュアルを参照してください。

15.2 コネクタのインストール

次の手順に従って、コネクタをインストールします。

- 1 Sentinel プラグイン Web サイトから、希望するコネクタをダウンロードします。
- 2 `https://<IP address>:8443` で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。
- 3 ツールバーで [アプリケーション] をクリックしてから、[アプリケーション] をクリックします。
- 4 [コントロールセンターの起動] をクリックして Sentinel コントロールセンターを起動します。
- 5 ツールバーで、[イベントソースの管理] > [ライブビュー] の順に選択し、[ツール] > [プラグインのインポート] の順にクリックします。

- 6 **ステップ 1** でダウンロードしたコネクタファイルをブラウザして選択してから、**[次へ]** をクリックします。
- 7 残りのプロンプトに従った後、**[終了]** をクリックします。

コネクタを環境設定するには、[Sentinel プラグイン Web サイト](#)にある、特定のコネクタのマニュアルを参照してください。

16 インストールの検証

次のいずれかを実行することにより、インストールが成功したかどうかを判断することができます。

- ◆ Sentinel のバージョンを確認する：

```
/etc/init.d/sentinel version
```

- ◆ Sentinel サービスが実行中かどうか、FIPS モードと非 FIPS モードのどちらで動作しているかを確認する：

```
/etc/init.d/sentinel status
```

- ◆ Web サービスが実行中であるかどうかを確認する：

```
netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
```

デフォルトのポート番号は 8443 です。

- ◆ Sentinel Web インタフェースにアクセスする：

1. サポートされている Web ブラウザを起動します。

2. Sentinel Web インタフェースの URL を指定する：

```
https://<IP_Address/DNS_Sentinel_server:8443>
```

「IP_Address_Sentinel_server」は Sentinel サーバの IP アドレスまたは DNS 名であり、「8443」は Sentinel サーバのデフォルトポートです。

3. インストール時に指定した管理者名とパスワードでログインします。デフォルトのユーザー名は admin です。

IV Sentinel の環境設定

このセクションでは、Sentinel および付属プラグインの環境設定について説明します。

- ◆ 99 ページの第 17 章「時刻の設定」
- ◆ 103 ページの第 18 章「インストール後の環境設定の変更」
- ◆ 105 ページの第 19 章「付属プラグインの環境設定」
- ◆ 107 ページの第 20 章「既存の Sentinel インストール環境を FIPS 140-2 モードにする」
- ◆ 109 ページの第 21 章「FIPS 140-2 モードでの Sentinel の運用」

17 時刻の設定

イベントの時刻は、Sentinel におけるイベントの処理には不可欠のものです。これはリアルタイム処理だけでなく、レポートや監査のためにも重要です。このセクションでは、Sentinel における時刻の意味、時刻の設定方法、およびタイムゾーンの取り扱いについて説明します。

- ◆ 99 ページのセクション 17.1 「Sentinel における時刻について」
- ◆ 101 ページのセクション 17.2 「Sentinel における時刻の設定」
- ◆ 101 ページのセクション 17.3 「イベントの遅延時間限度の環境設定」
- ◆ 101 ページのセクション 17.4 「タイムゾーンの処理」

17.1 Sentinel における時刻について

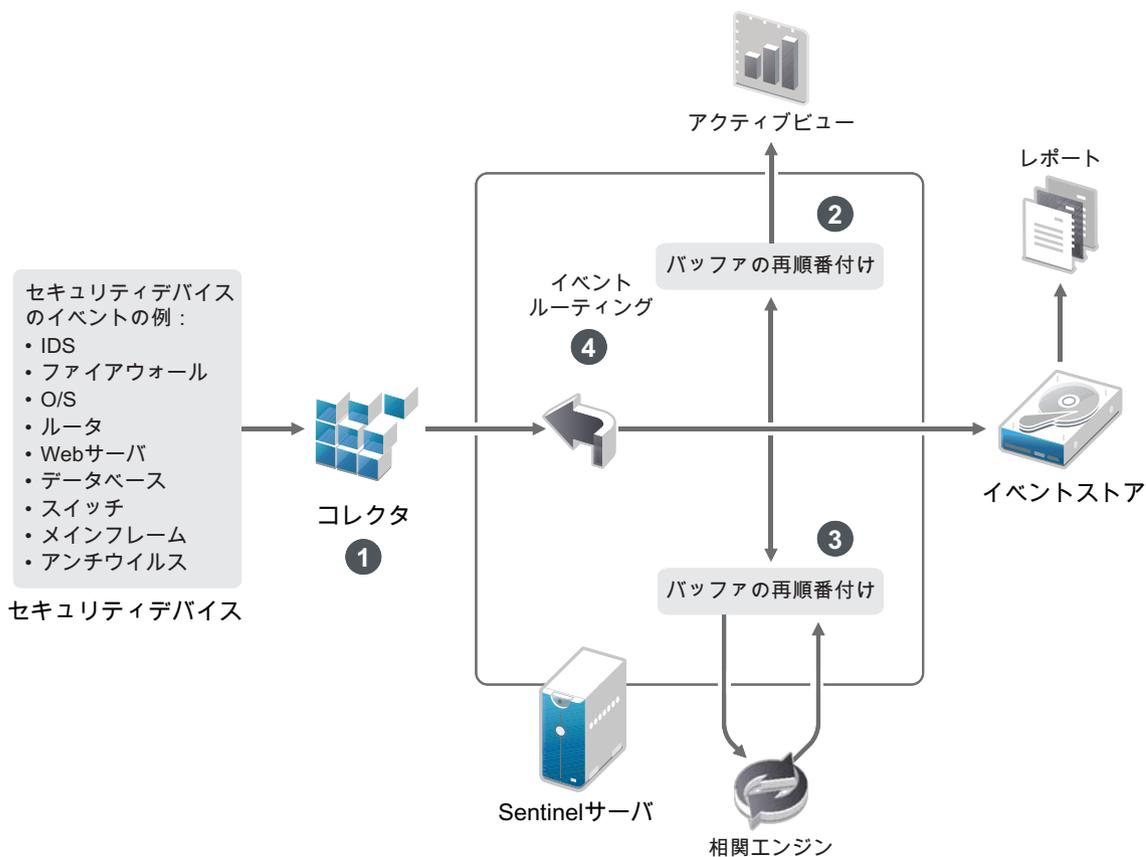
Sentinel は、ネットワーク全体に分散するいくつかのプロセスで構成される分散システムです。また、イベントソースによって多少の遅延が発生する可能性があります。これに対応するために、Sentinel プロセスは、イベントを処理する前に、イベントを時間順に並び替えます。

どのイベントにも 3 つの時刻フィールドがあります。

- ◆ **イベント時刻**：これは、すべての分析エンジン、検索、レポートなどで使用されるイベント時刻です。
- ◆ **Sentinel 処理時刻**：Sentinel がデバイスからデータを収集した時刻で、この時刻はコレクタマネージャのシステム時間から取得されます。
- ◆ **オブザーバイイベント時刻**：デバイスがデータに書き込んだタイムスタンプ。データに書き込まれたタイムスタンプは必ずしも信頼できるとは限らず、Sentinel 処理時刻と大きく異なっていることもあります。たとえば、デバイスがデータをバッチ処理で送信するとします。

次の図は、Sentinel がこれをどのように処理するのかを示しています。

図 17-1 Sentinel の時刻



1. デフォルトでは、イベント時刻は Sentinel 処理時刻に設定されます。しかし、オブザーバイベント時刻を利用でき、それが信頼に値するのであれば、イベント時刻がオブザーバイベント時刻と一致するのが理想的です。デバイス時刻を利用でき、正確で、コレクタが正しく解析できるのであれば、データ収集を【信頼イベントソース時刻】に設定するのが最善です。コレクタは、オブザーバイベント時刻に合うようにイベント時刻を設定します。
2. イベント時刻がサーバ時刻の前後 5 分以内であるイベントは、アクティブビューによって普通に処理されます。イベント時刻が 5 分以上進んでいるイベントは、アクティブビューには表示されませんが、イベントストアには挿入されます。イベント時刻が 5 分以上進んでいるイベントと過去 24 時間以内のイベントは、チャートには表示されますが、チャートのイベントデータには表示されません。これらのイベントをイベントストアから取得するには、ドリルダウン操作が必要です。
3. 関連エンジンはイベントを時間順に処理することができるように、イベントは 30 秒間隔でソートされます。イベント時刻がサーバ時刻よりも 30 秒を超えて古い場合、関連エンジンはイベントを処理しません。
4. イベント時刻がコレクタマネージャシステム時刻より 5 分を超えて古い場合、Sentinel はイベントを直接イベントストアにルーティングし、関連、アクティブビュー、セキュリティインテリジェンスなどのリアルタイムシステムはバイパスします。

17.2 Sentinel における時刻の設定

相関エンジンは、時間順に並べられたイベントのストリームを処理し、イベント内のパターンおよびストリーム内の時系列パターンを検出します。しかし、時々、イベントを生成するデバイスについてログメッセージに時刻が組み込まれないことがあります。Sentinel で時刻を正しく取り扱えるように設定するには、次の 2 つの方法があります。

- ◆ コレクタマネージャで NTP を設定し、イベントソースマネージャのイベントソース上で [信頼イベントソース時刻] の選択を解除します。Sentinel は、イベント時刻のソースとしてコレクタマネージャを使用します。
- ◆ イベントソースマネージャのイベントソース上で [信頼イベントソース時刻] を選択します。Sentinel は、ログメッセージの時刻を正しい時刻として使用します。

この設定をイベントソース上で変更するには：

- 1 [イベントソースの管理] にログインします。
詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Accessing Event Source Management](#)」を参照してください。
- 2 時刻の設定を変更するイベントソースを右クリックしてから、[編集] を選択します。
- 3 [全般] タブの下の [Trust Event Source] オプションを選択または選択解除します。
- 4 [OK] をクリックして変更内容を保存します。

17.3 イベントの遅延時間限度の環境設定

Sentinel がイベントソースからイベントを受け取る時に、イベントが生成された時間と Sentinel がそれを処理した時間の間で遅延が生じる場合があります。Sentinel は大きな遅延が生じたイベントを別個のパーティションに保存します。多くのイベントで長時間の遅延が生じている場合、それはイベントソースが正しく環境設定されていないことを示している場合があります。Sentinel は遅延が生じているイベントを処理しようとするため、Sentinel のパフォーマンスが低下することもあります。遅延が生じているイベントが正しくない環境設定の結果である可能性があるため、保存が望ましくない場合があります。そのため、Sentinel では、着信イベントでの受け入れ可能な遅延限度を設定できます。イベントルータはこの遅延限度を超えたイベントをドロップします。configuration.properties ファイル内の以下のプロパティで遅延限度を指定します。

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

リストを定期的に Sentinel サーバログファイルに記録することもできます。このファイルには、指定したしきい値を超えたイベントの受信元のイベントソースが示されます。この情報をログ記録するには、configuration.properties ファイル内の以下のプロパティでしきい値を指定します。

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

17.4 タイムゾーンの処理

分散環境では、タイムゾーンの処理が複雑になる場合があります。たとえば、あるタイムゾーンにイベントソースがあり、別のタイムゾーンにコレクタマネージャがあり、また別のタイムゾーンにバックエンドの Sentinel サーバがあり、さらに別のタイムゾーンでクライアントがデータを表示している場合などです。さらに夏時間や、設定されているタイムゾーンをレポートしないイベント

ソース (すべての Syslog ソースなど) を考慮すると、処理を必要とする問題は多くあります。Sentinel は、イベントが実際に発生した時刻を正しく示し、これらのイベントを同じタイムゾーンまたは別のタイムゾーンの他のイベントと比較することを可能にする柔軟性を備えています。

一般的に、イベントソースがタイムスタンプをレポートする方法は 3 通りあります。

- ◆ イベントソースが UTC で時刻をレポートする場合。たとえば、Windows イベントログの標準的なイベントはすべて、常に UTC でレポートされます。
- ◆ イベントソースがローカル時刻でレポートを行い、タイムスタンプにタイムゾーン情報が含まれている場合。たとえば、RFC3339 に従ってタイムスタンプを構成するイベントソースはすべて、オフセットとしてタイムゾーンを含みます。他のソースはアメリカ/ニューヨークなどの長いタイムゾーン ID、または EST などの短いタイムゾーン ID をレポートするため、不一致や不適切な解決などによる問題が発生する場合があります。
- ◆ イベントソースがローカル時刻でレポートし、タイムゾーン情報を含まない場合。残念ながら、とてもよく使われる Syslog フォーマットはこの形です。

最初の方法では、イベントが発生した絶対 UTC 時刻を計算できるため (時刻同期プロトコルが使用されていると想定)、そのイベントの時刻を他の世界中のイベントソースと容易に比較できます。ただし、イベントが発生したときのローカル時刻は自動的に判断できません。このため、Sentinel では、イベントソースのタイムゾーンを手動で設定できるようになっています。これは、イベントソースマネージャでイベントソースノードを編集して、適切なタイムゾーンを指定することにより可能です。この情報は [DeviceEventTime] や [EventTime] の計算には影響しませんが、[ObserverTZ] フィールドに取り込まれ、[ObserverTZHour] などの多様な [ObserverTZ] フィールドの計算に使用されます。これらのフィールドは、常にローカル時刻で示されます。

2 つめの方法では、長い形式のタイムゾーン ID またはオフセットが使用されている場合、UTC に変換して絶対的な標準 UTC 時刻 ([DeviceEventTime] に格納される) を取得できますが、ローカル時刻の [ObserverTZ] フィールドも計算できます。短い形式のタイムゾーン ID が使用されている場合、不一致が発生する可能性があります。

3 つめの方法では、Sentinel が UTC 時刻を正しく計算できるよう、影響を受けるすべてのソースのイベントソースタイムゾーンを管理者が手動で設定する必要があります。イベントソースマネージャでイベントソースノードを編集してタイムゾーンを正しく指定していない場合、[DeviceEventTime] (および、多くの場合は [EventTime]) が正しくない可能性があり、[ObserverTZ] および関連するフィールドも正しくない場合があります。

一般的に、特定のイベントソース (たとえば、Microsoft Windows など) 用のコレクタは、イベントソースからのタイムスタンプの形式が判明しているため、それに応じて調整を行います。イベントソースがローカル時刻でレポートし、タイムスタンプに常にタイムゾーンが含まれているのでない限り、イベントソースマネージャでイベントソースノードすべてに対して手動でタイムゾーンを設定することをお勧めします。

イベントソースからのタイムスタンプ情報は、コレクタおよびコレクタマネージャ上で処理されます。[DeviceEventTime] および [EventTime] は UTC として格納され、[ObserverTZ] フィールドはイベントソースのローカル時刻の文字列として格納されます。この情報はコレクタマネージャから Sentinel サーバに送信され、イベントストア内に格納されます。コレクタマネージャおよび Sentinel サーバが配置されたタイムゾーンは、このプロセスにも格納されるデータにも影響しません。ただし、クライアントが Web ブラウザでイベントを確認する場合、UTC の [EventTime] は Web ブラウザによってローカル時刻に変換されます。そのため、クライアントには、すべてのイベントがローカルのタイムゾーンで示されます。ユーザがソースのローカル時刻を知りたい場合は、[ObserverTZ] フィールドで詳細を確認できます。

18 インストール後の環境設定の変更

Sentinel のインストール後に、有効なライセンスキーを入力したり、パスワードを変更したり、割り当てられたポートを変更したりする場合は、`configure.sh` スクリプトを実行してこれらの変更を行います。スクリプトは、`/opt/novell/sentinel/setup` フォルダにあります。

- 1 以下のコマンドを使用して、Sentinel をシャットダウンします。

```
rcsentinel stop
```

- 2 コマンドラインで次のコマンドを指定して、`configure.sh` スクリプトを実行します。

```
./configure.sh
```

- 3 Sentinel の標準環境設定を実行するには、「1」を指定します。カスタム環境設定を実行する場合は、「2」を指定します。

- 4 スペースキーを押して使用許諾契約を確認します。

- 5 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

インストールパッケージをロードするのに数秒かかることがあります。

- 6 デフォルトの評価版ライセンスキーを使用するには、「1」を入力します。

または

購入した Sentinel ライセンスキーを入力するには、「2」を入力します。

- 7 管理者ユーザ `admin` の既存のパスワードをそのまま使用するかどうか決定します。

- ◆ 既存のパスワードをそのまま使用するには、「1」を入力してから [ステップ 8](#) に進みます。
- ◆ 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、[ステップ 8](#) に進みます。

`admin` ユーザは、Sentinel Web コンソールから管理タスク（他のユーザアカウントの作成など）を実行するために使用される ID です。

- 8 データベースユーザ `dbauser` の既存のパスワードをそのまま使用するかどうか決定します。

- ◆ 既存のパスワードをそのまま使用するには、「1」を入力してから [ステップ 9](#) に進みます。
- ◆ 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、[ステップ 9](#) に進みます。

`dbauser` アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。

- 9 アプリケーションユーザ `appuser` の既存のパスワードをそのまま使用するかどうか決定します。

- ◆ 既存のパスワードをそのまま使用するには、「1」を入力してから [ステップ 10](#) に進みます。
- ◆ 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、[ステップ 10](#) に進みます。

`appuser` アカウントは、Sentinel java プロセスがデータベースと接続を確立し、データをやり取りするために使用する内部 ID です。ここで入力したパスワードはデータベースタスクの実行に使用されます。

- 10 目的の番号を入力してから新しいポート番号を指定して、Sentinel サービスのポート割り当てを変更します。
- 11 ポートを変更してから「7」を指定し、完了します。
- 12 内部データベースのみを使用してユーザを認証するには、「1」を入力します。
または
ドメインで LDAP ディレクトリを設定している場合に、LDAP ディレクトリ認証を使用してユーザを認証するには、「2」を入力します。
デフォルト値は 1 です。

19 付属プラグインの環境設定

Sentinel には、Sentinel リリース時点で利用可能なデフォルトの Sentinel プラグインがプリインストールされています。

本章では、付属プラグインの環境設定を行う方法について説明します。

- ◆ 105 ページのセクション 19.1 「プリインストールプラグインの表示」
- ◆ 105 ページのセクション 19.2 「データコレクションの環境設定」
- ◆ 105 ページのセクション 19.3 「ソリューションパックの環境設定」
- ◆ 106 ページのセクション 19.4 「アクションとインテグレータの環境設定」

19.1 プリインストールプラグインの表示

Sentinel にプリインストールされているプラグインのリストを表示することができます。プラグインのバージョンや他のメタデータも見ることができ、利用可能なプラグインが最新バージョンかどうかを確認するのに役立ちます。

Sentinel サーバにインストールされているプラグインを表示するには：

- 1 <https://<IP アドレス>:8443> で、Sentinel Web インタフェースに管理者としてログインします。8443 は Sentinel サーバのデフォルトポートです。
- 2 [プラグイン] > [カタログ] の順にクリックします。

19.2 データコレクションの環境設定

データコレクションに関する Sentinel の環境設定については、『[NetIQ Sentinel Administration Guide](#)』の「[Collecting and Routing Event Data](#)」を参照してください。

19.3 ソリューションパックの環境設定

Sentinel には、分析に関する多数のニーズに合わせて、導入後直ちに使用可能なさまざまなコンテンツが同梱されています。コンテンツの多くは、プリインストールされた Sentinel Core ソリューションパックおよび ISO 27000 Series のソリューションパックの一部です。詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Using Solution Packs](#)」を参照してください。

ソリューションパックによって、コンテンツを1つのユニットとして扱われるコントロールやポリシーセットに分類したり、グループにまとめたりすることができます。この導入後直ちに使用可能なコンテンツを提供するためにソリューションパックのコントロールがプリインストールされていますが、これらのコントロールは Sentinel Web コンソールを使用して、形式に沿って実装またはテストする必要があります。

Sentinel の実装が設計どおりに機能していることをある程度厳密に確認する場合は、ソリューションパックに組み込まれた形式的検証プロセスを使用できます。この検証プロセスでは、他のソリューションパックのコントロールの実装とテストを行う場合と全く同じように、ソリューション

パックコントロールを実装およびテストします。このプロセスの一環として、実装担当者とテスト担当者が作業を完了したことを検証します。次に、これらの検証が監査証跡に含められ、特定のコントロールが正しく展開されたことを確認できます。

検証プロセスは、ソリューションマネージャを使用して実施できます。詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Installing and Managing Solution Packs](#)」を参照してください。

19.4 アクションとインテグレータの環境設定

付属プラグインの環境設定については、[Sentinel プラグイン Web サイト](#)にある特定のプラグインマニュアルを参照してください。

20 既存の Sentinel インストール環境を FIPS 140-2 モードにする

本章では、Sentinel の既存インストール環境を FIPS 140-2 モードにする方法について説明します。

注：Sentinel が `/opt/novell/sentinel` ディレクトリにインストールされていることを前提としています。コマンドは `novell` ユーザとして実行する必要があります。

- ◆ [107 ページのセクション 20.1 「Sentinel サーバを FIPS 140-2 モードで実行する」](#)
- ◆ [107 ページのセクション 20.2 「リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする」](#)

20.1 Sentinel サーバを FIPS 140-2 モードで実行する

Sentinel サーバを FIPS 140-2 モードで実行できるようにするには：

- 1 Sentinel サーバにログインします。
- 2 `novell` ユーザ (`su novell`) に切り替えます。
- 3 Sentinel の `bin` ディレクトリを参照します。
- 4 `convert_to_fips.sh` スクリプトを実行して、画面の指示に従います。
- 5 [109 ページの第 21 章「FIPS 140-2 モードでの Sentinel の運用」](#) に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

20.2 リモートコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする

FIPS 140-2 モードで実行している Sentinel サーバとの接続で FIPS 認定通信を使用する場合は、リモートのコレクタマネージャおよび関連エンジンで FIPS 140-2 モードを有効にする必要があります。

リモートのコレクタマネージャまたは関連エンジンを FIPS 140-2 モードで動作させるには：

- 1 リモートのコレクタマネージャまたは関連エンジンのシステムにログインします。
- 2 `novell` ユーザ (`su novell`) に切り替えます。
- 3 `bin` ディレクトリを参照します。デフォルトの場所は `/opt/novell/sentinel/bin` です。
- 4 `convert_to_fips.sh` スクリプトを実行して、画面の指示に従います。
- 5 [109 ページの第 21 章「FIPS 140-2 モードでの Sentinel の運用」](#) に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

21 FIPS 140-2 モードでの Sentinel の運用

本章では、FIPS 140-2 モードの Sentinel の環境設定と運用について説明します。

- ◆ 109 ページのセクション 21.1「Advisor サービスを FIPS 140-2 モードで実行するように環境設定する」
- ◆ 109 ページのセクション 21.2「分散検索を FIPS 140-2 モードで実行するように環境設定する」
- ◆ 111 ページのセクション 21.3「LDAP 認証を FIPS 140-2 モードで実行するように環境設定する」
- ◆ 111 ページのセクション 21.4「リモートコレクタマネージャおよび関連エンジンのサーバ証明書を更新」
- ◆ 112 ページのセクション 21.5「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」
- ◆ 118 ページのセクション 21.6「証明書を FIPS キーストアデータベースにインポートする」
- ◆ 118 ページのセクション 21.7「Sentinel を非 FIPS モードに戻す」

21.1 Advisor サービスを FIPS 140-2 モードで実行するように環境設定する

Advisor サービスはセキュアな HTTPS 接続を使用して、Advisor サーバからフィードフォームをダウンロードします。サーバがセキュア通信に使用している証明書が、Sentinel FIPS キーストアデータベースに追加される必要があります。

リソース管理データベースに正常に登録されたことを検証するには：

- 1 [Advisor サーバ](#)から証明書をダウンロードして、そのファイルに `advisor.cer` という名前を付けて保存します。
- 2 Advisor サーバ証明書を Sentinel FIPS キーストアにインポートします。
証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

21.2 分散検索を FIPS 140-2 モードで実行するように環境設定する

このセクションでは、分散検索を FIPS 140-2 モードで実行するように環境設定する方法について説明します。

シナリオ 1: ソースとターゲットの両方の Sentinel サーバが FIPS 140-2 モードである

FIPS 140-2 モードで実行されている複数の Sentinel サーバにわたって分散検索を実行できるようにするには、セキュア通信で使用する証明書を FIPS キーストアに追加する必要があります。

- 1 分散検索ソースコンピュータにログインします。
- 2 証明書ディレクトリを参照します。

```
cd <sentinel_install_directory>/config
```

- 3 ソース証明書 (sentinel.cer) をターゲットコンピュータの一時的な場所にコピーします。
- 4 ソース証明書をターゲットの Sentinel FIPS キーストアにインポートします。
証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。
- 5 分散検索ターゲットコンピュータにログインします。
- 6 証明書ディレクトリを参照します。

```
cd /etc/opt/novell/sentinel/config
```

- 7 ターゲット証明書 (sentinel.cer) をソースコンピュータの一時的な場所にコピーします。
- 8 ターゲットシステム証明書をソースの Sentinel FIPS キーストアにインポートします。
- 9 ソースコンピュータとターゲットコンピュータの両方で Sentinel サービスを再起動します。

シナリオ 2: ソース Sentinel サーバが非 FIPS モードであり、ターゲット Sentinel サーバが FIPS 140-2 モードである

ソースコンピュータの Web サーバキーストアを証明書フォーマットに変換してから、証明書をターゲットコンピュータにエクスポートする必要があります。

- 1 分散検索ソースコンピュータにログインします。
- 2 証明書 (.cer) 形式で、Web サーバキーストアを作成します。

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -  
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass  
password -file <certificate_name.cer>
```

- 3 分散検索ソース証明書 (Sentinel.cer) を分散検索ターゲットコンピュータの一時的な場所にコピーします。
- 4 分散検索ターゲットコンピュータにログインします。
- 5 ソース証明書をターゲットの Sentinel FIPS キーストアにインポートします。
証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。
- 6 ターゲットコンピュータの Sentinel サービスを再起動します。

シナリオ 3: ソース Sentinel サーバが FIPS モードであり、ターゲット Sentinel サーバが非 FIPS モードである

- 1 分散検索ターゲットコンピュータにログインします。
- 2 証明書 (.cer) 形式で、Web サーバキーストアを作成します。

```
<sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -  
keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass  
password -file <certificate_name.cer>
```

- 3 証明書を分散検索ソースコンピュータの一時的な場所にコピーします。
- 4 ターゲット証明書をソースの Sentinel FIPS キーストアにインポートします。
証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。
- 5 ソースコンピュータの Sentinel サービスを再起動します。

21.3 LDAP 認証を FIPS 140-2 モードで実行するように環境設定する

FIPS 140-2 モードで実行している Sentinel サーバに対して LDAP 認証を設定するには：

- 1 LDAP 管理者から LDAP サーバ証明書入手します。または、コマンドを使用することもできます。たとえば、

```
openssl s_client -connect <LDAP server IP>:636
```

コマンド実行後に返されるテキスト (BEGIN 行と END 行の間) をファイルにコピーします。

- 2 LDAP サーバ証明書を Sentinel FIPS キーストアにインポートします。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

- 3 Sentinel Web コンソールに管理者の役割のユーザとしてログインして、LDAP 認証の設定を続行します。

詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Configuring LDAP Authentication](#)」を参照してください。

注：FIPS 140-2 モードで実行している Sentinel サーバの LDAP 認証の設定は、`/opt/novell/sentinel/setup` ディレクトリにある `ldap_auth_config.sh` スクリプトを実行することによっても行えます。

21.4 リモートコレクタマネージャおよび関連エンジンのサーバ証明書の更新

既存のリモートコレクタマネージャおよびリモート関連エンジンを FIPS 140-2 モードで実行している Sentinel サーバと通信するように設定するには、リモートシステムを FIPS 140-2 モードに変換するか、またはリモートシステムに対して Sentinel サーバ証明書を更新してコレクタマネージャまたは関連エンジンを非 FIPS モードのままにしておきます。FIPS モードのリモートコレクタマネージャは、FIPS モードをサポートしないイベントソース、またはまだ FIPS が使用可能になっていない Sentinel コネクタのうちのいずれかを必要とするイベントソースと連携できない可能性があります。

リモートのコレクタマネージャまたは関連エンジンで FIPS140-2 モードを有効にしない場合は、最新の Sentinel サーバ証明書をリモートシステムにコピーして、コレクタマネージャまたは関連エンジンが Sentinel サーバと通信できるようにする必要があります。

リモートのコレクタマネージャまたは関連エンジンの Sentinel サーバ証明書を更新するには：

- 1 リモートのコレクタマネージャまたは関連エンジンのコンピュータにログインします。
- 2 `novell` ユーザ (`su novell`) に切り替えます。
- 3 `bin` ディレクトリを参照します。デフォルトの場所は `/opt/novell/sentinel/bin` です。
- 4 `updateServerCert.sh` スクリプトを実行して、画面の指示に従います。

21.5 Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する

このセクションでは、さまざまな Sentinel プラグインを FIPS 140-2 モードで実行するための設定について説明します。

注： Sentinel が `/opt/novell/sentinel` ディレクトリにインストールされていることを前提としています。コマンドは `novell` ユーザとして実行する必要があります。

- ◆ 112 ページのセクション 21.5.1 「エージェントマネージャコネクタ」
- ◆ 113 ページのセクション 21.5.2 「データベース (JDBC) コネクタ」
- ◆ 113 ページのセクション 21.5.3 「Sentinel Link コネクタ」
- ◆ 114 ページのセクション 21.5.4 「Syslog コネクタ」
- ◆ 115 ページのセクション 21.5.5 「Windows イベント (WMI) コネクタ」
- ◆ 116 ページのセクション 21.5.6 「Sentinel Link インテグレータ」
- ◆ 117 ページのセクション 21.5.7 「LDAP インテグレータ」
- ◆ 117 ページのセクション 21.5.8 「SMTP インテグレータ」
- ◆ 117 ページのセクション 21.5.9 「FIPS 140-2 モードの Sentinel で FIPS 非対応コネクタを使用する」

21.5.1 エージェントマネージャコネクタ

エージェントマネージャイベントソースサーバのネットワーク設定時に [暗号化 (HTTPS)] オプションを選択した場合にのみ、以下の手順に従ってください。

エージェントマネージャコネクタを FIPS 140-2 モードで実行するように設定するには：

- 1 エージェントマネージャイベントソースサーバを追加または編集します。[セキュリティ] ウィンドウが表示されるまで、設定画面を進めていきます。詳細については、『*Agent Manager Connector Guide*』を参照してください。
- 2 [クライアント認証のタイプ] フィールドでオプションを 1 つ選択します。クライアント認証タイプによって、SSL エージェントマネージャイベントソースサーバがデータの送信を試行しているエージェントマネージャイベントソースの ID をどの程度厳密に検証するかが決まります。
 - ◆ **開く：** エージェントマネージャエージェントから着信するすべての SSL 接続を許可します。クライアント証明書の検証または認証は行いません。
 - ◆ **厳密：** 証明書が有効な X.509 証明書であるかを検証し、クライアント証明書がイベントソースサーバによって信頼されていることも確認します。新規ソースは Sentinel に明示的に追加する必要があります (そうすることで、不正なソースが認証されていないデータを送信できないようにします)。

[**厳密**] オプションの場合、各新規エージェントマネージャクライアントの証明書を Sentinel FIPS キーストアにインポートする必要があります。Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

注: FIPS 140-2 モードでは、エージェントマネージャイベントソースサーバは Sentinel サーバキーを使用するため、サーバキーペアのインポートは必須ではありません。

- 3 エージェントでサーバ認証が有効になっている場合、コネクタが展開されている場所に応じて、Sentinel サーバ証明書リモートコレクタマネージャ証明書を信頼するようにエージェントも設定する必要があります。

Sentinel サーバ証明書がある場所: `/etc/opt/novell/sentinel/config/sentinel.cer`

リモートコレクタマネージャ証明書がある場所: `/etc/opt/novell/sentinel/config/rcm.cer`

注: 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、エージェントマネージャエージェントが適切な証明書ファイルを信頼していなければなりません。

21.5.2 データベース (JDBC) コネクタ

データベース接続の設定時に [SSL] オプションを選択した場合にのみ、以下の手順に従います。

データベースコネクタを FIPS 140-2 モードで実行するように設定するには:

- 1 コネクタを設定する前に、データベースサーバから証明書をダウンロードし、`database.cert` というファイル名にして、Sentinel サーバの `/etc/opt/novell/sentinel/config` ディレクトリに保存します。
詳細については、各データベースのマニュアルを参照してください。
- 2 証明書を Sentinel FIPS キーストアにインポートします。
証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。
- 3 続けてコネクタの設定を行います。

21.5.3 Sentinel Link コネクタ

Sentinel Link イベントソースサーバのネットワーク設定時に「暗号化 (HTTPS)」オプションを選択している場合にのみ、以下の手順に従ってください。

Sentinel Link コネクタを FIPS 140-2 モードで実行するように設定するには:

- 1 Sentinel Link イベントソースサーバを追加または編集します。[セキュリティ] ウィンドウが表示されるまで、設定画面を進めていきます。詳細については、『*Sentinel Link Connector Guide*』を参照してください。

2 [クライアント認証のタイプ] フィールドでオプションを1つ選択します。クライアント認証タイプによって、SSL Sentinel Link イベントソースサーバがデータの送信を試行している Sentinel Link イベントソース (Sentinel Link インテグレータ) の ID をどの程度厳密に検証するかが決まります。

- ◆ **開く** : クライアント (Sentinel Link インテグレータ) から着信するすべての SSL 接続を許可します。インテグレータ証明書の検証または認証は行いません。
- ◆ **厳密** : インテグレータ証明書が有効な X.509 証明書であるかを検証し、インテグレータ証明書がイベントソースサーバによって信頼されているかも確認します。詳細については、各データベースのマニュアルを参照してください。

[**厳密**] オプションの場合 :

- ◆ Sentinel Link インテグレータが FIPS 140-2 モードで動作しているときは、`/etc/opt/novell/sentinel/config/sentinel.cer` ファイルを送信側の Sentinel マシンから受信側の Sentinel マシンにコピーする必要があります。証明書を受信側の Sentinel FIPS キーストアにインポートします。

注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、適切なカスタム証明書ファイルをインポートする必要があります。

- ◆ Sentinel Link インテグレータが非 FIPS モードで動作しているときは、カスタムインテグレータ証明書を受信側の Sentinel FIPS キーストアにインポートする必要があります。

注 : 送信者が Sentinel ログマネージャ (非 FIPS モード) であり、受信者が FIPS 140-2 モードの Sentinel である場合、送信者がインポートするサーバ証明書は受信者の Sentinel マシンの `/etc/opt/novell/sentinel/config/sentinel.cer` ファイルです。

Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

注 : FIPS 140-2 モードでは、Sentinel Link イベントソースサーバは Sentinel サーバのキーペアを使用します。サーバのキーペアのインポートは必須ではありません。

21.5.4 Syslog コネクタ

Syslog イベントソースサーバのネットワーク設定時に「SSL」プロトコルを選択している場合にのみ、以下の手順に従ってください。

Syslog コネクタを FIPS 140-2 モードで実行するように設定するには :

- 1 Syslog イベントソースサーバを追加または編集します。[ネットワーク] ウィンドウが表示されるまで、設定画面での作業を進めていきます。詳細については、『*Syslog Connector Guide*』を参照してください。
- 2 [設定] をクリックします。

- 3 [クライアント認証のタイプ] フィールドでオプションを1つ選択します。クライアント認証タイプによって、SSL Syslog イベントソースサーバがデータの送信を試行している Syslog イベントソースの ID をどの程度厳密に検証するかが決まります。

- ◆ **開く** : クライアント (イベントソース) から着信するすべての SSL 接続を許可します。クライアント証明書の検証または認証は行いません。
- ◆ **厳密** : 証明書が有効な X.509 証明書であるかを検証し、クライアント証明書がイベントソースサーバによって信頼されていることも確認します。新規ソースは Sentinel に明示的に追加する必要があります (そうすることで、不正なソースがデータを Sentinel に送信できないようにします) 。

[**厳密**] オプションの場合、Syslog クライアントの証明書を Sentinel FIPS キーストアにインポートする必要があります。

Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

注 : FIPS 140-2 モードでは、Syslog イベントソースサーバは Sentinel サーバのキーペアを使用します。サーバのキーペアのインポートは必須ではありません。

- 4 Syslog クライアントでサーバ認証が有効になっている場合、コネクタが展開されている場所に応じて、クライアントは Sentinel サーバ証明書リモートコレクタマネージャ証明書を信頼する必要があります。

Sentinel サーバ証明書ファイルは /etc/opt/novell/sentinel/config/sentinel.cer にあります。

リモートコレクタマネージャ証明書ファイルは /etc/opt/novell/sentinel/config/rcm.cer にあります。

注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、クライアントが適切な証明書ファイルを信頼していなければなりません。

21.5.5 Windows イベント (WMI) コネクタ

Windows イベント (WMI) コネクタを FIPS 140-2 モードで実行するように設定するには :

- 1 Windows イベントコネクタを追加または編集します。[セキュリティ] ウィンドウが表示されるまで、設定画面を進めていきます。詳細については、『*Windows Event (WMI) Connector Guide*』を参照してください。
- 2 [設定] をクリックします。
- 3 [クライアント認証のタイプ] フィールドでオプションを1つ選択します。クライアント認証タイプによって、Windows イベントコネクタがデータの送信を試行しているクライアント Windows イベント収集サービス (WECS) の ID をどの程度厳密に検証するかが決まります。
 - ◆ **開く** : クライアント WECS から着信するすべての SSL 接続を許可します。クライアント証明書の検証または認証は行いません。
 - ◆ **厳密** : 証明書が有効な X.509 証明書であるかを検証し、クライアント WECS 証明書が CA によって署名されているかも確認します。新規ソースは明示的に追加する必要があります (そうすることで、不正なソースがデータを Sentinel に送信できないようにします) 。

[**厳密**] オプションの場合、クライアント WECS の証明書を Sentinel FIPS キーストアにインポートする必要があります。Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

注: FIPS 140-2 モードでは、Windows イベントソースサーバは Sentinel サーバのキーペアを使用します。サーバのキーペアのインポートは必須ではありません。

- 4 Windows クライアントでサーバ認証が有効になっている場合、コネクタが展開されている場所に応じて、クライアントは Sentinel サーバ証明書カリモートコレクタマネージャ証明書を信頼する必要があります。

Sentinel サーバ証明書ファイルは /etc/opt/novell/sentinel/config/sentinel.cer にあります。

リモートコレクタマネージャ証明書ファイルは /etc/opt/novell/sentinel/config/rcm.cer にあります。

注: 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、クライアントが適切な証明書ファイルを信頼していなければなりません。

- 5 イベントソースを自動的に同期する場合、または Active Directory 接続を使用しているイベントソースのリストを生成する場合は、Active Directory サーバ証明書を Sentinel FIPS キーストアにインポートする必要があります。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

21.5.6 Sentinel Link インテグレータ

Sentinel Link インテグレータのネットワーク設定時に「**暗号化 (HTTPS)**」オプションを選択している場合にのみ、以下の手順に従ってください。

Sentinel Link インテグレータを FIPS 140-2 モードで実行するように設定するには:

- 1 Sentinel Link インテグレータが FIPS 140-2 モードであるときは、サーバ認証が必須になります。インテグレータインスタンスを設定する前に、Sentinel Link サーバ証明書を Sentinel FIPS キーストアにインポートしてください。

- ◆ **Sentinel Link コネクタが FIPS 140-2 モードである場合:**

コネクタが Sentinel サーバに展開されている場合、/etc/opt/novell/sentinel/config/sentinel.cer ファイルを受信側 Sentinel マシンから送信側 Sentinel マシンにコピーする必要があります。

コネクタがリモートコレクタマネージャに展開されている場合は、/etc/opt/novell/sentinel/config/rcm.cer ファイルを受信側のリモートコレクタマネージャマシンから受信側の Sentinel マシンにコピーする必要があります。

証明書を送信側の Sentinel FIPS キーストアにインポートします。

注: 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、適切なカスタム証明書ファイルをインポートする必要があります。

- ◆ Sentinel Link コネクタが非 FIPS モードである場合:

カスタム Sentinel Link サーバ証明書を送信側の Sentinel FIPS キーストアにインポートします。

注: Sentinel Link インテグレータが FIPS 140-2 モードであり、Sentinel Link コネクタが非 FIPS モードのときは、コネクタにあるカスタムサーバのキーペアを使用してください。内部サーバのキーペアは使用しないでください。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

- 2 続けてインテグレータインスタンスの設定を行います。

注: FIPS 140-2 モードでは、Sentinel Link インテグレータは Sentinel サーバのキーペアを使用します。インテグレータのキーペアのインポートは必須ではありません。

21.5.7 LDAP インテグレータ

LDAP インテグレータを FIPS 140-2 モードで実行するように設定するには:

- 1 インテグレータインスタンスを設定する前に、LDAP サーバから証明書をダウンロードし、`ldap.cert` というファイル名にして、Sentinel サーバの `/etc/opt/novell/sentinel/config` ディレクトリに保存します。

たとえば、次のように入力します。

```
openssl s_client -connect <LDAP server IP>:636
```

コマンド実行後に返されるテキスト (BEGIN 行と END 行の間) をファイルにコピーします。

- 2 証明書を Sentinel FIPS キーストアにインポートします。

証明書のインポートについて詳しくは、[118 ページの「証明書を FIPS キーストアデータベースにインポートする」](#)を参照してください。

- 3 続けてインテグレータインスタンスの設定を行います。

21.5.8 SMTP インテグレータ

SMTP インテグレータは、2011.1r2 以降のバージョンで FIPS 140-2 をサポートしています。設定の変更は必要ありません。

21.5.9 FIPS 140-2 モードの Sentinel で FIPS 非対応コネクタを使用する

このセクションでは、FIPS 非対応コネクタを FIPS 140-2 モードの Sentinel サーバで使用方法について説明します。FIPS をサポートしないソースがある場合、またはご使用の環境で非 FIPS コネクタからイベントを収集する場合に、この方法をお勧めします。

FIPS 140-2 モードの Sentinel サーバで非 FIPS コネクタを使用するには:

- 1 非 FIPS モードのコレクタマネージャをインストールして、FIPS 140-2 モードの Sentinel サーバに接続します。

詳細については、[63 ページのパート III 「Sentinel のインストール」](#) を参照してください。

- 2 非 FIPS コネクタを明確に非 FIPS リモートコレクタマネージャに展開します。

注： 監査コネクタやファイルコネクタなどの非 FIPS コネクタを、FIPS 140-2 モードの Sentinel サーバに接続している非 FIPS リモートコレクタマネージャ上で展開する場合に発生する、既知の問題があります。これらの既知の問題の詳細については、[Sentinel 7.1 リリースノート](#) を参照してください。

21.6 証明書を FIPS キーストアデータベースにインポートする

証明書を Sentinel FIPS キーストアデータベースに挿入して、その証明書を所有するコンポーネントから Sentinel へのセキュア (SSL) 通信を確立する必要があります。FIPS 140-2 モードが Sentinel で有効になっている場合、通常どおり Sentinel ユーザインタフェースを使用して証明書をアップロードすることはできません。証明書を FIPS キーストアデータベースに手動でインポートする必要があります。

リモートコレクタマネージャに展開されたコネクタを使用しているイベントソースの場合、証明書を中央 Sentinel サーバではなく、リモートコレクタマネージャの FIPS キーストアデータベースにインポートする必要があります。

証明書を FIPS キーストアデータベースにインポートするには：

- 1 証明書ファイルを Sentinel サーバまたはリモートコレクタマネージャの一時的な場所にコピーします。
- 2 Sentinel の bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。
- 3 次のコマンドを実行して、証明書を FIPS キーストアデータベースにインポートし、画面の指示に従ってください。

```
./convert_to_fips.sh -i <certificate file path>
```

- 4 Sentinel サーバまたはリモートコレクタマネージャを再起動するようプロンプトが表示されたら、「yes」または「y」と入力します。

21.7 Sentinel を非 FIPS モードに戻す

このセクションでは、Sentinel およびそのコンポーネントを非 FIPS モードに戻す方法について説明します。

- ◆ [118 ページのセクション 21.7.1 「Sentinel サーバを非 FIPS モードに戻す」](#)
- ◆ [119 ページのセクション 21.7.2 「リモートコレクタマネージャまたはリモート関連エンジンを非 FIPS モードに戻す」](#)

21.7.1 Sentinel サーバを非 FIPS モードに戻す

FIPS 140-2 モードで実行している Sentinel サーバを非 FIPS モードに戻すことができるのは、Sentinel サーバを FIPS 140-2 モードにする前に Sentinel サーバのバックアップを取ってある場合のみです。

注: Sentinel サーバを非 FIPS モードに戻すと、FIPS 140-2 モード実行に変換した後のイベント、インシデントデータ、および Sentinel サーバに対して行われた設定変更は失われます。Sentinel システムは非 FIPS モードの最後の復元ポイントに復元されます。後で使用するを考えて、現在のシステムのバックアップを取ってから、非 FIPS モードに戻すようにしてください。

Sentinel サーバを非 FIPS モードに戻すには:

- 1 Sentinel サーバに root ユーザでログインします。
- 2 novell ユーザに切り替えます。
- 3 Sentinel の bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。
- 4 次のコマンドを実行して、Sentinel サーバを非 FIPS モードに戻し、画面の指示に従ってください。

```
./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
```

たとえば、non-fips2013012419111359034887.tar.gz がバックアップファイルである場合は、次のコマンドを実行します。

```
./backup_util.sh -f non-fips2013012419111359034887.tar.gz -m 'restore'
```

- 5 Sentinel サーバを再起動します。

21.7.2 リモートコレクタマネージャまたはリモート関連エンジンを非 FIPS モードに戻す

リモートコレクタマネージャまたはリモート関連エンジンを非 FIPS モードに戻すことができます。

リモートコレクタマネージャまたはリモート関連エンジンを非 FIPS モードに戻すには:

- 1 リモートコレクタマネージャまたはリモート関連エンジンのシステムにログインします。
- 2 novell ユーザ (su novell) に切り替えます。
- 3 bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。
- 4 revert_to_nonfips.sh スクリプトを実行して、画面の指示に従います。
- 5 リモートコレクタマネージャまたはリモート関連エンジンを再起動します。

V Sentinel のアップグレード

このセクションでは、Sentinel およびコンポーネントのアップグレードについて説明します。

- ◆ [123 ページの第 22 章「実装チェックリスト」](#)
- ◆ [125 ページの第 23 章「前提条件」](#)
- ◆ [127 ページの第 24 章「従来の Sentinel インストールのアップグレード」](#)
- ◆ [133 ページの第 25 章「Sentinel アプライアンスのアップグレード」](#)
- ◆ [139 ページの第 26 章「アップグレード後の環境設定」](#)
- ◆ [141 ページの第 27 章「Sentinel プラグインのアップグレード」](#)

22 実装チェックリスト

Sentinel をアップグレードする前に、以下のチェックリストを確認して、正しくアップグレードされるようにしてください。

表 22-1 実装チェックリスト

<input type="checkbox"/>	タスク	参照先
<input type="checkbox"/>	Sentinel およびそのコンポーネントのインストール先となるコンピュータが所定の要件を満たしていることを確認します。	NetIQ Sentinel 技術情報 Web サイト
<input type="checkbox"/>	サポートされているオペレーティングシステムのリリースノートで既知の問題を確認します。	SUSE リリースノート
<input type="checkbox"/>	Sentinel リリースノートで新しい機能と既知の問題を確認します。	Sentinel リリースノート
<input type="checkbox"/>	「前提条件」で説明されているタスクを完了します。	125 ページの第 23 章「前提条件」

23 前提条件

- ◆ 125 ページのセクション 23.1 「カスタム環境設定情報の保存」
- ◆ 125 ページのセクション 23.2 「Change Guardian の統合」
- ◆ 125 ページのセクション 23.3 「Sentinel 7.1.1 より前のバージョンの場合の前提条件」

23.1 カスタム環境設定情報の保存

カスタム環境設定パラメータの値を `server.conf` ファイルで設定している場合は、その値を別のファイルに保存してからアップグレードを実行します。

カスタム環境設定情報を保存するには、次の手順を実行します。

- 1 Sentinel サーバに `novell` ユーザでログインし、`/etc/opt/novell/sentinel/config/` ディレクトリに移動します。
- 2 `server-custom.conf` という名前の設定ファイルを作成し、このファイルにカスタム設定パラメータを追加します。
- 3 (オプション) Netflow コレクタなど、Sentinel の他のコンポーネントについて、類似するカスタム設定ファイルを作成します。たとえば、`netflow-collector-custom.conf` です。

Sentinel は、アップグレード中にこれらの設定ファイル内の保存されたカスタム構成を適用します。

23.2 Change Guardian の統合

Sentinel には、Change Guardian 4.2 以降との互換性があります。Sentinel からイベントを受信するには、まず、Change Guardian サーバをバージョン 4.2 以降にアップグレードする必要があります。これにより、Sentinel はアップグレード後の Change Guardian からイベントを引き続き受信するようになります。

23.3 Sentinel 7.1.1 より前のバージョンの場合の前提条件

Sentinel 7.1.1 以降には MongoDB バージョン 2.4.1 が含まれています。MongoDB 2.4 では、データベース内の重複したユーザ名を削除することが必要です。Sentinel 7.1.1 より前のバージョンからアップグレードする場合は、重複しているユーザがないかを確認して、あれば削除してください。

重複したユーザを識別するには、以下のステップを実行します。

- 1 Sentinel 7.1 以前のサーバに `novell` ユーザでログインします。
- 2 以下のディレクトリに変更します。

```
cd opt/novell/sentinel/3rdparty/mongodb/bin
```
- 3 重複したユーザを検証するには、以下のコマンドを実行します。

```
./mongo --port 27017 --host "localhost"
```

```
use analytics
```

```
db.system.users.find().count()
```

count が 1 より大きい場合、重複したユーザーであることを示しています。

重複したユーザを削除するには、以下のステップを実行します。

- 1 以下のコマンドを実行して、ユーザをリストします。

```
db.system.users.find().pretty()
```

このコマンドによって、ユーザと重複したエントリがリストされます。リスト内の最初のユーザはオリジナルのユーザです。最初のユーザは保持し、リスト内のその他のユーザを削除する必要があります。

- 2 以下のコマンドを実行して、重複したユーザを削除します。

```
db.system.users.remove({ _id : ObjectId("object_ID") })
```

- 3 以下のコマンドを実行して、重複したユーザが削除されたかどうかを検証します。

```
db.system.users.find().pretty()
```

- 4 データベースの管理者ユーザに切り替えます。

```
use admin
```

- 5 **ステップ 1** から**ステップ 3** を繰り返して、管理データベース内の重複した dbusers を確認して削除します。

24 従来の Sentinel インストールのアップグレード

- ◆ 127 ページのセクション 24.1 「Sentinel のアップグレード」
- ◆ 128 ページのセクション 24.2 「非 root ユーザとしての Sentinel のアップグレード」
- ◆ 130 ページのセクション 24.3 「コレクタマネージャまたは関連エンジンのアップグレード」

24.1 Sentinel のアップグレード

次の手順に従って、Sentinel サーバをアップグレードします。

- 1 環境設定をバックアップしてから、ESM エクスポートを作成します。
データのバックアップの詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。
- 2 (条件付き) server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。
詳しくは、『[NetIQ Sentinel Administration Guide](#)』の「[Maintaining Custom Settings in XML Files](#)」を参照してください。
- 3 [NetIQ ダウンロード Web サイト](#) から最新のインストーラをダウンロードします。
- 4 Sentinel をアップグレードするサーバに root としてログインします。
- 5 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

```
tar xfz <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

- 6 インストールファイルを抽出したディレクトリに移動します。
- 7 次のコマンドを指定して、Sentinel をアップグレードします。

```
./install-sentinel
```
- 8 指定の言語でインストールを進めるには、言語の横の番号を選択します。
エンドユーザの使用許諾契約が、選択した言語で表示されます。
- 9 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。
- 10 インストールスクリプトで、古いバージョンの製品が存在していることが検出され、製品をアップグレードするかどうかを指定するよう求められます。アップグレードを続行するには、「y」を押します。
すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。
- 11 Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

- 12 クライアントコンピュータ上の Java Web Start キャッシュを消去してから、最新バージョンの Sentinel アプリケーションを使用します。

javaws -clearcache コマンドを使用するか、Java コントロールセンターを使用して、Java Web Start キャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xml を参照してください。

- 13 (条件による) PostgreSQL データベースがメジャーバージョンにアップグレードされた場合 (8.0 から 9.0 や 9.0 から 9.1 など)、PostgreSQL データベースから古い PostgreSQL ファイルを消去してください。PostgreSQL データベースがアップグレードされたかどうかについて詳しくは、『Sentinel リリースノート』を参照してください。

- 13a novell ユーザに切り替えます。

```
su novell
```

- 13b bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

- 13c 次のコマンドを使用して、古い PostgreSQL ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

- 14 (条件による) Sentinel 7.1.1 以前のバージョンからアップグレードしている場合、インストーラはデフォルトではセキュリティインテリジェンス (SI) データを移行しません。Sentinel 7.1.1 以前のバージョンから SI データを移行するには、次のようにして SI データの移行を手動で使用可能にします。

- 14a novell ユーザに切り替えます。

```
su novell
```

- 14b /etc/opt/novell/sentinel/config/server.xml ファイルを開きます。

- 14c [BaseliningRuntime] コンポーネントセクションに次のプロパティを追加します。

```
<property name="baselining.migration.check">true</property>
```

- 14d Sentinel サーバを再起動します。

- 15 コレクタマネージャシステムおよび関連エンジンシステムをアップグレードするには、[130 ページのセクション 24.3 「コレクタマネージャまたは関連エンジンのアップグレード」](#) を参照してください。

24.2 非 root ユーザとしての Sentinel のアップグレード

組織のポリシーによって、root としての Sentinel のフルアップグレードが実行できない場合は、別のユーザとして Sentinel をアップグレードできます。このアップグレードでは、いくつかの手順を root ユーザとして実行してから、root ユーザによって作成された別のユーザとして Sentinel をアップグレードします。

- 1 環境設定をバックアップしてから、ESM エクスポートを作成します。

データのバックアップ方法については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。

2 (条件付き) server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳細については、『*NetIQ Sentinel Administration Guide*』の「[Backing Up and Restoring Data](#)」を参照してください。

3 [NetIQ ダウンロード Web サイト](#) からインストールファイルをダウンロードします。

4 コマンドラインで次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

```
tar -zxvf <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

5 Sentinel をアップグレードするサーバに root としてログインします。

6 Sentinel インストールファイルから squashfs RPM を抽出します。

7 Sentinel サーバに squashfs をインストールします。

```
rpm -Uvh <install_filename>
```

8 次のコマンドを指定して、新しく作成された、root でない novell ユーザに変更します : novell:
su novell

9 (条件による) インタラクティブアップグレードを実行するには :

9a 次のコマンドを指定します。

```
./install-sentinel
```

デフォルトの場所がない Sentinel をアップグレードするには、コマンドと一緒に --location オプションを指定します。例 :

```
./install-sentinel --location=/foo
```

9b [ステップ 11](#) に進みます。

10 (条件による) サイレントアップグレードを実行するには、次のコマンドを指定します。

```
./install-sentinel -u <response_file>
```

インストールは、レスポンスファイルに格納された値を使用して進行します。Sentinel のアップグレードが完了します。

11 アップグレードに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

12 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、アップグレードを続行します。

アップグレードですべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

13 Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

14 クライアントコンピュータ上の Java Web Start キャッシュを消去してから、最新バージョンの Sentinel アプリケーションを使用します。

javaws -clearcache コマンドを使用するか、Java コントロールセンターを使用して、Java Web Start キャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xml を参照してください。

- 15 (条件による) PostgreSQL データベースがメジャーバージョンにアップグレードされた場合 (8.0 から 9.0 や 9.0 から 9.1 など)、PostgreSQL データベースから古い PostgreSQL ファイルを消去してください。PostgreSQL データベースがアップグレードされたかどうかについて詳しくは、『Sentinel リリースノート』を参照してください。

15a novell ユーザに切り替えます。

```
su novell
```

15b bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

15c 次のコマンドを使用して、古い PostgreSQL ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

- 16 (条件による) Sentinel 7.1.1 以前のバージョンからアップグレードしている場合、インストーラはデフォルトではセキュリティインテリジェンス (SI) データを移行しません。Sentinel 7.1.1 以前のバージョンから SI データを移行するには、次のようにして SI データの移行を手動で使用可能にします。

16a novell ユーザに切り替えます。

```
su novell
```

16b /etc/opt/novell/sentinel/config/server.xml ファイルを開きます。

16c [BaseliningRuntime] コンポーネントセクションに次のプロパティを追加します。

```
<property name="baselining.migration.check">true</property>
```

16d Sentinel サーバを再起動します。

24.3 コレクタマネージャまたは関連エンジンのアップグレード

次の手順に従って、コレクタマネージャおよび関連エンジンをアップグレードします：

- 1 環境設定をバックアップしてから、ESM エクスポートを作成します。
詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。
- 2 Sentinel の Web インタフェースに管理者の役割を持つユーザとしてログインします。
- 3 [ダウンロード] を選択します。
- 4 コレクタマネージャのインストーラセクションで [インストーラのダウンロード] をクリックします。
- 5 それぞれのコレクタマネージャサーバまたは関連エンジンサーバにインストーラファイルを保存します。
- 6 ファイルを一時的な場所にコピーします。
- 7 ファイルの内容を抽出します。
- 8 次のスクリプトを実行します。

コレクタマネージャの場合：

```
./install-cm
```

関連エンジンの場合：

```
./install-ce
```

- 9 画面の説明に従って、インストールを完了します。
- 10 (条件による) カスタムインストールの場合、次のコマンドを実行して、Sentinel サーバ、コレクタマネージャ、および関連エンジン間で環境設定を同期します。

```
/opt/novell/sentinel/setup/configure.sh
```


25 Sentinel アプライアンスのアップグレード

本章では、Sentinel アプライアンス、およびコレクタマネージャアプライアンスと関連エンジンアプライアンスをアップグレードする手順について説明します。

- ◆ 133 ページのセクション 25.1 「zypper を使用したアプライアンスのアップグレード」
- ◆ 135 ページのセクション 25.2 「WebYaST を使用したアプライアンスのアップグレード」
- ◆ 136 ページのセクション 25.3 「SMT を使用したアプライアンスのアップグレード」

25.1 zypper を使用したアプライアンスのアップグレード

zypper patch を使用してアプライアンスをアップグレードするには：

- 1 環境設定をバックアップしてから、ESM エクスポートを作成します。
詳細については、『*NetIQ Sentinel Administration Guide*』の「[Backing Up and Restoring Data](#)」を参照してください。
- 2 (条件付き) server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。
詳しくは、『*NetIQ Sentinel Administration Guide*』の「[Maintaining Custom Settings in XML Files](#)」を参照してください。
- 3 アプライアンスコンソールに root ユーザでログインします。
- 4 次のコマンドを実行します。

```
/usr/bin/zypper patch
```
- 5 (条件による) Sentinel 7.0.1 以前のバージョンをアップグレードしている場合は、「1」を入力して、Novell から NetIQ へのベンダーの変更を受諾します。
- 6 (条件による) Sentinel 7.2 より前のバージョンをアップグレードしている場合、インストーラは一部のアプライアンスパッケージの従属関係を解決する必要があることを伝えるメッセージを表示します。従属パッケージのインストールを解除する場合は、「1」と入力します。
- 7 (条件による) Sentinel 7.2 以降をアップグレードしている場合、インストーラは ncgOverlay アーキテクチャの変更を示すオプションを表示します。適切なオプションを入力して、アーキテクチャの変更を受諾します。
- 8 「Y」と入力して続行します。
- 9 使用許諾契約書の条項を確認し、「yes」と入力します。
- 10 Sentinel アプライアンスを再起動します。
- 11 (条件による) Sentinel をカスタムポートにインストールした場合や、コレクタマネージャまたは関連エンジンが FIPS モードの場合は、次のコマンドを実行します。

```
/opt/novell/sentinel/setup/configure.sh
```
- 12 Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

- 13** クライアントコンピュータ上の Java Web Start キャッシュを消去してから、最新バージョンの Sentinel アプリケーションを使用します。

javaws -clearcache コマンドを使用するか、Java コントロールセンターを使用して、Java Web Start キャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xml を参照してください。

- 14** (条件による) PostgreSQL データベースがメジャーバージョンにアップグレードされた場合 (8.0 から 9.0 や 9.0 から 9.1 など)、PostgreSQL データベースから古い PostgreSQL ファイルを消去してください。PostgreSQL データベースがアップグレードされたかどうかについて詳しくは、『Sentinel リリースノート』を参照してください。

- 14a** novell ユーザに切り替えます。

```
su novell
```

- 14b** bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

- 14c** 次のコマンドを使用して、古い postgresql ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

- 15** (条件による) Sentinel 7.1.1 以前のバージョンからアップグレードしている場合、インストーラはデフォルトではセキュリティインテリジェンス (SI) データを移行しません。Sentinel 7.1.1 以前のバージョンから SI データを移行するには、次のようにして SI データの移行を手動で使用可能にします。

- 15a** novell ユーザに切り替えます。

```
su novell
```

- 15b** /etc/opt/novell/sentinel/config/server.xml ファイルを開きます。

- 15c** [BaseliningRuntime] コンポーネントセクションに次のプロパティを追加します。

```
<property name="baselining.migration.check">true</property>
```

- 15d** Sentinel サーバを再起動します。

- 16** (条件による) コレクタマネージャまたは関連エンジンをアップグレードするには、[ステップ 3](#) から [ステップ 11](#) までを実行します。

25.2 WebYaST を使用したアプライアンスのアップグレード

WebYaST を使用したアプライアンスのアップグレードは、Sentinel のバージョンが 7.3.2 以降の場合、または「[Sentinel 7.3.2 リリースノート](#)」の説明にあるように手動で NetIQ Change Guardian RPM をアップグレードした場合にのみ実行できます。

Sentinel 7.3.2 より前のバージョンからアプライアンスをアップグレードする場合、アップグレードを完了するためにユーザによる操作が必要となるため、zypper コマンドラインユーティリティを使用する必要があります。WebYaST では、必要とされるユーザとのやり取りを実行できません。zypper を使用したアプライアンスのアップグレードについては、[133 ページのセクション 25.1 「zypper を使用したアプライアンスのアップグレード」](#)を参照してください。

- 1 Sentinel アプライアンスに管理者の役割を持つユーザとしてログインします。
- 2 環境設定をバックアップしてから、ESM エクスポートを作成します。
詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。
- 3 (条件付き) server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳しくは、『[NetIQ Sentinel Administration Guide](#)』の「[Maintaining Custom Settings in XML Files](#)」を参照してください。
- 4 Sentinel アプライアンスをアップグレードする場合は、[アプライアンス] をクリックして WebYaST を起動します。
- 5 コレクタマネージャまたは関連エンジンアプライアンスをアップグレードする場合は、コレクタマネージャまたは関連エンジンのコンピュータの URL をポート 4984 を使用して指定し (https://<IP_address>:4984)、WebYaST を起動します。ここで、<IP_address> はコレクタマネージャまたは関連エンジンの IP アドレスを指します。[ステップ 6 からステップ 10](#) までを行います。
- 6 (条件による) アプライアンスの自動更新をまだ登録していない場合は、登録します。
詳細については、[85 ページのセクション 13.3.3 「アップデートの登録」](#)を参照してください。
アプライアンスが登録されていない場合、Sentinel はアプライアンスが登録されていないことを示す黄色い警告を表示します。
- 7 アップデートがあるかどうかを確認するには、[更新] をクリックします。
利用可能な更新が表示されます。
- 8 更新を選択して適用します。
更新が完了するまで数分かかる場合があります。更新が成功すると、WebYaST のログインページが表示されます。
アプライアンスをアップグレードする前に、WebYaST は Sentinel サービスを自動的に停止します。アップグレードが完了した後で、このサービスを手動で再開する必要があります。
- 9 Web インタフェースを使用して Sentinel サービスを再開します。
詳細については、[87 ページのセクション 13.4 「WebYaST を使用したサーバの起動と停止」](#)を参照してください。
- 10 (条件による) Sentinel をカスタムポートにインストールした場合や、コレクタマネージャまたは関連エンジンが FIPS モードの場合は、次のコマンドを実行します。

```
/opt/novell/sentinel/setup/configure.sh
```

- 11 Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。
- 12 クライアントコンピュータ上の Java Web Start キャッシュを消去してから、最新バージョンの Sentinel アプリケーションを使用します。

javaws -clearcache コマンドを使用するか、Java コントロールセンターを使用して、Java Web Start キャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xml を参照してください。

- 13 (条件による) PostgreSQL データベースがメジャーバージョンにアップグレードされた場合 (8.0 から 9.0 や 9.0 から 9.1 など)、PostgreSQL データベースから古い PostgreSQL ファイルを消去してください。PostgreSQL データベースがアップグレードされたかどうかについて詳しくは、『Sentinel リリースノート』を参照してください。

- 13a novell ユーザに切り替えます。

```
su novell
```

- 13b bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

- 13c 次のコマンドを使用して、古い postgresql ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

- 14 (条件による) Sentinel 7.1.1 以前のバージョンからアップグレードしている場合、インストーラはデフォルトではセキュリティインテリジェンス (SI) データを移行しません。Sentinel 7.1.1 以前のバージョンから SI データを移行するには、次のようにして SI データの移行を手動で使用可能にします。

- 14a novell ユーザに切り替えます。

```
su novell
```

- 14b /etc/opt/novell/sentinel/config/server.xml ファイルを開きます。

- 14c [BaseliningRuntime] コンポーネントセクションに次のプロパティを追加します。

```
<property name="baselining.migration.check">true</property>
```

- 14d Sentinel サーバを再起動します。

25.3 SMT を使用したアプライアンスのアップグレード

インターネットに直接アクセスできない保護された環境でアプライアンスを実行する必要がある場合は、Subscription Management Tool (SMT) でアプライアンスを設定することができます。これにより、アプライアンスを使用可能な最新のバージョンにアップグレードできます。

- 1 アプライアンスが SMT で設定されていることを確認します。

詳細については、[86 ページのセクション 13.3.4 「SMT でのアプライアンスの設定」](#) を参照してください。

- 2 環境設定をバックアップしてから、ESM エクスポートを作成します。

詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。

3 (条件付き) server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳しくは、『[NetIQ Sentinel Administration Guide](#)』の「[Maintaining Custom Settings in XML Files](#)」を参照してください。

4 アプライアンスコンソールに root ユーザでログインします。

5 アップグレード用にリポジトリを更新します。

```
zypper ref -s
```

6 アプライアンスがアップグレードに対して有効であることを確認します。

```
zypper lr
```

7 (オプション) アプライアンスの使用可能な更新を確認します。

```
zypper lu
```

8 (オプション) アプライアンスの使用可能な更新を含むパッケージを確認します。

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

9 アプライアンスを更新します。

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

10 アプライアンスを再起動します。

```
rcsentinel restart
```

11 (条件による) Sentinel をカスタムポートにインストールした場合や、コレクタマネージャまたは関連エンジンが FIPS モードの場合は、次のコマンドを実行します。

```
/opt/novell/sentinel/setup/configure.sh
```

12 (条件による) コレクタマネージャまたは関連エンジンをアップグレードするには、[ステップ 4](#) から [ステップ 11](#) までを実行します。

26 アップグレード後の環境設定

この章では、アップグレード後の環境設定について説明します。

- ◆ [139 ページのセクション 26.1「JDBC DB2 ドライバの追加」](#)
- ◆ [139 ページのセクション 26.2「Sentinel アプライアンスのデータフェデレーションプロパティの設定」](#)

26.1 JDBC DB2 ドライバの追加

Sentinel のアップグレード後には、次の手順を実行して、正しい JDBC ドライバを追加し、データ収集とデータ同期が行われるように JDBC ドライバを設定します。

- 1 /opt/novell/sentinel/lib フォルダに、お使いの DB2 データベースのバージョンに適する IBM DB2 JDBC ドライバ (db2jcc-*.jar) のバージョンをコピーします。
- 2 ドライバファイルに必要な所有権およびアクセス権を設定してください。
- 3 データ収集用にこのドライバを構成します。詳細については、[データベースコネクタのマニュアル](#)を参照してください。

26.2 Sentinel アプライアンスのデータフェデレーションプロパティの設定

Sentinel アプライアンスのアップグレード後に、次の手順を実行して、複数の NIC が構成されている環境でデータフェデレーションがエラーを表示しないようにします。

- 1 許可リクエストサーバで、次のプロパティを /etc/opt/novell/sentinel/config/configuration.properties ファイルに追加します。
sentinel.distsearch.console.ip=< 許可リクエストの IP アドレスの 1 つ >
- 2 データソースサーバで、次のプロパティを /etc/opt/novell/sentinel/config/configuration.properties ファイルに追加します。
sentinel.distsearch.target.ip=< データソースの IP アドレスの 1 つ >
- 3 Sentinel を再起動します。
rcsentinel restart
- 4 許可リクエストサーバにログインし、[統合] をクリックします。追加するデータソースが既に存在する場合、それを削除してから、ステップ 2 で指定した IP アドレスの 1 つを使用して追加しなおします。
同じように、許可リクエストを、ステップ 1 で指定した IP アドレスを使用して追加します。

27 Sentinel プラグインのアップグレード

Sentinel のインストール環境をアップグレードしても、最新版の Sentinel との互換性がないプラグインはアップグレードされません。

ソリューションパックを含め、新しい Sentinel プラグインや更新された Sentinel プラグインは、頻繁に [Sentinel プラグイン Web サイト](#) にアップロードされます。最新のバグフィックス、マニュアルの更新、およびプラグインの拡張機能入手するには、プラグインの最新バージョンをダウンロードしてインストールしてください。プラグインのインストールについては、それぞれのプラグインのマニュアルを参照してください。

VI 高可用性のための Sentinel の展開

本付録では、NetIQ Sentinel を「アクティブ-パッシブ高可用性」モードでインストールする方法を説明します。このモードでインストールすると、ハードウェアやソフトウェアの障害が起きたときに、Sentinel を冗長クラスタノードにフェールオーバーさせることができます。お客様の Sentinel 環境における高可用性と障害復旧の実装に関する詳しい情報は、[NetIQ テクニカルサポート](#) [ト](#)にお問い合わせください。

注：高可用性 (HA) 環境設定は Sentinel サーバでのみサポートされています。しかし、コレクタマネージャと相関エンジンは Sentinel HA サーバとも通信できます。

- ◆ [145 ページの第 28 章「概念」](#)
- ◆ [147 ページの第 29 章「システム要件」](#)
- ◆ [149 ページの第 30 章「インストールと環境設定」](#)
- ◆ [165 ページの第 31 章「高可用性の Sentinel のアップグレード」](#)
- ◆ [171 ページの第 32 章「バックアップと復元」](#)

28 概念

高可用性とは、システムを現実的な範囲でできる限り継続的に利用できるようにすることを目的とした一つの設計方法論です。システム障害やシステム保守といったダウンタイムの原因を極力排除し、実際に発生してしまったダウンタイムイベントの検出とそこからの回復にかかる時間を最小限に抑えることを意図しています。より高度な可用性を実現するために、具体的には、ダウンタイムイベントの検出とそこからの回復を迅速に行う自動化された処理方法が必要となります。

高可用性の詳細については、『[SUSE High Availability Guide](#)』を参照してください。

- ◆ [145 ページのセクション 28.1「外部システム」](#)
- ◆ [145 ページのセクション 28.2「共有ストレージ」](#)
- ◆ [146 ページのセクション 28.3「サービスの監視」](#)
- ◆ [146 ページのセクション 28.4「フェンシング」](#)

28.1 外部システム

Sentinel は、さまざまなサービスに依存しながらさまざまなサービスを提供する、複合的な多層アプリケーションです。また、複数の外部サードパーティシステムとも連動して、データ収集、データ共有、およびインシデント修正を行います。ほとんどの HA ソリューションでは高可用性を持たせるサービス間の依存関係を実装者が宣言できますが、これはクラスタ自体で動作しているサービスにしか適用されません。イベントソースなどの Sentinel 外部のシステムは、組織が必要とする可用性に合わせて別個に構成する必要があり、フェールオーバーなどのために Sentinel が一時的に利用不能になった場合でも状況を適切に処理できるように設定されている必要があります。アクセス権限が厳しく制限されている場合（たとえばサードパーティシステムと Sentinel との間でのデータの送信または受信（あるいはその両方）に認証済みセッションを使用する場合など）、どのクラスタノードからでもセッションを受け入れ、どのクラスタノードに対してもセッションを開始できるようにサードパーティシステムを設定する必要があります（そのためには Sentinel を仮想 IP で設定する必要があります）。

28.2 共有ストレージ

すべての HA クラスタには、ノードに障害が起きた場合でもアプリケーションデータを別のノードにすばやく移動できるような、何らかの形式の共有ストレージが必要です。ストレージそのものが高可用性を備えていなければならない、これは通常ファイバチャネルネットワークを使用してクラスタノードに接続するストレージエリアネットワーク (SAN) の技術を採用することによって実現されます。他のシステムは NAS(Network Attached Storage)、iSCSI、または共有ストレージのリモートマウントを可能にするその他のテクノロジーを使用します。共有ストレージの最も重要な要件は、クラスタが障害の発生したクラスタノードから新しいクラスタノードへストレージをきちんと移動できるということです。

注：iSCSI の場合は、ハードウェアがサポートする最大のメッセージ転送単位 (MTU) を使用してください。MTU を大きくすることで、ストレージのパフォーマンスが向上します。ストレージのレイテンシと帯域幅が推奨値より遅いと、Sentinel で問題が生じる可能性があります。

Sentinel における共有ストレージの使用には、2つの基本的なアプローチがあります。1つは、すべてのコンポーネント(アプリケーションバイナリ、環境設定、およびイベントデータ)を共有ストレージに置くという方法です。フェールオーバーになると、ストレージはプライマリノードからアンマウントされてバックアップノードに移動します。これで、共有ストレージから全体のアプリケーションと設定が読み込まれます。もう一つは、イベントデータを共有ストレージに保管し、アプリケーションバイナリと設定は各クラスタノードに配置するという方法です。フェールオーバーになると、イベントデータのみがバックアップノードに移動します。

どちらの方法にも長所と短所がありますが、2番目の方法では、Sentinel インストール環境で標準 FHS 準拠のインストールパスを使用でき、RPM パッケージの検証、ダウンタイムを最小限にするウォームパッチや再設定を行うことが可能です。

iSCSI 共有ストレージを使用し、アプリケーションバイナリと設定を各クラスタノードに配置するクラスタのインストールプロセスを、サンプルとして説明していきます。

28.3 サービスの監視

高可用性環境の重要な要素は、高可用であるべきリソースとそれに依存するリソースを監視するための、信頼できる安定した方法を確立することです。SLE HAE はリソースエージェントというコンポーネントを使用してそのような監視を実行します。リソースエージェントの役目は、各リソースの状況を知らせ、そのリソースを(要求に応じて)開始および停止することです。

リソースエージェントは監視対象のリソース状況を信頼できる情報として提供して、不要なダウンタイムが発生しないようにする必要があります。誤検出(リソースに障害が発生したと思われたが、実際には自力で回復したという場合など)によって実際には行う必要のないサービスマイグレーション(および関連するダウンタイム)が始まったり、検出漏れ(リソースは機能しているとリソースエージェントが報告したが、そのリソースは実際には正常に動作していないという場合など)によってサービスを適正に利用できなくなったりすることがあります。一方、サービスに対して外部監視を行うことは非常に難しいでしょう。たとえば、Web サービスポートは1つの単純な ping には応答するかもしれませんが、実際のクエリが発行されたときに正しいデータを提供できるとは限りません。多くの場合、本当に正確な測定値を取得するには、サービス自体に自己診断機能を組み込む必要があります。

このソリューションでは、主要なハードウェア、オペレーティングシステム、または Sentinel システム障害を監視することができる、基本 OCF リソースエージェントが Sentinel に装備されます。現時点では、Sentinel の外部監視機能は IP ポート試験に基づいており、これには読み取りに誤検出や検出漏れの可能性があります。弊社では、このコンポーネントの正確性を改善するために、時間をかけて Sentinel およびリソースエージェントの両方を改良することを計画しています。

28.4 フェンシング

HA クラスタ内では、クリティカルサービスを常時監視しており、障害発生時には別のノードでそのサービスが自動的に再起動するようになっています。しかし、この自動化によって問題が生じる可能性もあります。たとえば、プライマリノードで何らかの通信の問題が発生し、そのノード上で実行中のサービスが一見ダウンしているようでも、実際には実行が継続され、データを共有ストレージに書き込んでいるという場合です。このような場合に、バックアップノードで新たにサービスのセットが開始されると、容易にデータ破損が発生しかねません。

そうならないように、クラスタではフェンシングという方法が採用されています。これは、スプリットブレイン検出(SBD)およびSTONITH(Shoot The Other Node In The Head)を含むさまざまな技術の総称です。この主な目的は、共有ストレージにおけるデータ破損を防ぐことにあります。

29 システム要件

高可用性 (HA) インストール環境に対応できるようにクラスタリソースを割り振る場合、以下の要件を考慮してください。

- (条件による) HA アプライアンスインストールでは、有効なライセンス付きの Sentinel HA アプライアンスが使用可能であることを確認します。Sentinel HA アプライアンスは、以下のパッケージを含む ISO アプライアンスです。
 - ◆ SUSE Linux Enterprise Server (SLES) 11 SP3 オペレーティングシステム
 - ◆ SUSE Linux Enterprise Server High Availability Extension (SLES HAE) パッケージ
 - ◆ Sentinel ソフトウェア (HA rpm を含む)
- (条件による) 従来の HA インストールの場合、有効なライセンス付きの Sentinel インストーラ (TAR ファイル) と SUSE Linux High Availability Extension (SLE HAE) ISO イメージが使用可能なことを確認します。
- (条件による) SLESオペレーティングシステム(カーネルバージョン 3.0.101以降)を使用している場合、コンピュータにウォッチドッグドライバを手動でロードする必要があります。ご使用のコンピュータハードウェア用の適切なウォッチドッグドライバを見つけるには、ハードウェアベンダーに連絡してください。ウォッチドッグドライバをロードするには、以下を実行します。
 1. コマンドプロンプトで、以下のコマンドを実行し、現在のセッションでウォッチドッグドライバをロードします。

```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```
 2. /etc/init.d/boot.local ファイルに、次の行を追加して、毎ブート時にコンピュータが自動的にウォッチドッグドライバをロードするようにします：

```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```
- Sentinel サービスをホストする各クラスタノードが、37 ページの第 5 章「システム要件を満たす」に指定されている要件を満たしていることを確認します。
- Sentinel データおよびアプリケーションが使用できる十分な共有ストレージが確保されていることを確認します。
- フェールオーバー時にノードからノードに移動できるサービスに対して、仮想 IP アドレスが使用されていることを確認します。
- 共有ストレージデバイスが、37 ページの第 5 章「システム要件を満たす」に指定されているパフォーマンスおよびサイズ特性の要件を満たしていることを確認します。NetIQ は、標準 SUSE Linux VM を使用し、iSCSI Target を共有ストレージとして環境設定することを推奨します。
- お客様の環境で Sentinel を実行するためのリソース要件を満たしたクラスタノードが少なくとも 2 つあるようにします。NetIQ では、2 台の SUSE Linux VM を使用することを推奨します。
- クラスタノードが共有ストレージと通信する方式 (SAN 用の FibreChannel など) を作成しておきます。NetIQ では、iSCSI Target に接続するための専用 IP アドレスを推奨します。

- ❑ Sentinel の外部 IP アドレスの役割を果たす、クラスタ内のノード間で移行可能な仮想 IP があることを確認します。
- ❑ 各クラスタノードにつき内部クラスタ通信用の IP アドレスが少なくとも 1 つあることを確認します。NetIQ では単一のユニキャスト IP アドレスを推奨していますが、運用環境ではマルチキャストが好まれます。

30.1 初期セットアップ

Sentinel 用に記述されている要件およびローカルのお客様の要件に従って、コンピュータハードウェア、ネットワークハードウェア、ストレージハードウェア、オペレーティングシステム、ユーザアカウント、およびその他の基本的なシステムリソースを設定します。システムをテストして、正常に機能し安定していることを確認します。

次のチェックリストを使用して、初期セットアップと環境設定を行います。

	チェックリストの項目
<input type="checkbox"/>	各クラスタノードの CPU、RAM、およびディスク容量特性が、予想されるイベント発生率に基づいて、 37 ページの第 5 章「システム要件を満たす」 に定義されているシステム要件を満たしている必要があります。
<input type="checkbox"/>	ストレージノードのディスク容量と入出力特性は、予想されるイベント発生率、プライマリおよびセカンダリストレージのデータ保持ポリシーに基づいて、 37 ページの第 5 章「システム要件を満たす」 で定義されているシステム要件を満たしている必要があります。
<input type="checkbox"/>	Sentinel およびクラスタへのアクセスを制限するためにオペレーティングシステムのファイアウォールを設定する場合は、 55 ページの第 8 章「使用するポート」 を参照してください。ローカル構成やイベントデータを送信する送信元に応じて、どのポートを使用可能にする必要があるのか詳しく説明されています。
<input type="checkbox"/>	すべてのクラスタノードの時刻が同期されていることを確認します。NTP または類似のテクノロジーを使って、確認することができます。
<input type="checkbox"/>	<ul style="list-style-type: none">クラスタには、信頼できるホスト名解決が必要です。DNS 障害が発生してもクラスタが稼働を継続できるようにするために、すべての内部クラスタホスト名を /etc/hosts ファイルに入力しておきます。ループバック IP アドレスにホスト名を割り当てることのないようにします。オペレーティングシステムのインストール時にホスト名とドメイン名を設定する際に、[ホスト名をループバック IP に割り当てる] の選択を解除します。

NetIQ では、次の環境設定を推奨します。

- ♦ (条件による) 従来の HA インストールの場合：
 - ♦ SUSE Linux 11 SP3 クラスタノードの仮想マシンを 2 台
 - ♦ (条件による) GUI 設定が必要な場合は、X Windows をインストールできます。X なしで起動するようにブートスクリプトを設定すると (実行レベル 3)、必要な場合にのみ起動させることができます。
- ♦ (条件による) HA アプライアンスインストールの場合：HA ISO アプライアンスベースクラスタノードの仮想マシンを 2 台 HA ISO アプライアンスのインストールについて詳しくは、[80 ページのセクション 13.1.2「Sentinel のインストール」](#)を参照してください。
- ♦ ノードには、外部アクセス用に 1 つの NIC、iSCSI 通信用にもう 1 つの NIC が設定されます。
- ♦ SSH または同様の機能を介してリモートアクセスできるように、外部 NIC に IP アドレスを設定します。このサンプルでは、172.16.0.1 (node01) と 172.16.0.2 (node02) を使用します。
- ♦ 各ノードには、オペレーティングシステム、Sentinel のバイナリおよび設定データ、クラスタソフトウェア、一時スペースなどのために十分なディスク容量がなければなりません。SUSE Linux および SLE HAE のシステム要件、および Sentinel アプリケーション要件を参照してください。

- ◆ 1つの SUSE Linux 11 SP3 VM(共有ストレージ用に iSCSI Target を設定済み)
 - ◆ (条件による) GUI 設定が必要な場合は、X Windows をインストールできます。X なしで起動するようにブートスクリプトを設定すると (実行レベル 3)、必要な場合にのみ起動させることができます。
 - ◆ システムには2つの NIC が設定されます。1つは外部アクセス用で、もう1つは iSCSI 通信用です。
 - ◆ SSH または同様の機能を使用してリモートアクセスできるような IP アドレスを外部 NIC に設定します。たとえば、「172.16.0.3 (storage03)」のように入力します。
 - ◆ オペレーティングシステム、一時スペース、Sentinel データを保持する大容量の共有ストレージのための十分なスペース、および SBD パーティションのためのいくつかのスペースを、システムに確保してください。SUSE Linux システム要件および Sentinel イベントデータストレージ要件を参照してください。

注：運用クラスタでは、内部クラスタ通信用に、個々の NIC (おそらくは冗長性のために2個1組) でルーティング不可の内部 IP を使用できます。

30.2 共有ストレージのセットアップ

共有ストレージをセットアップして、そのストレージをクラスタノードごとにマウントします。FibreChannel と SAN を使用している場合は、物理的な接続と追加の環境設定を行うことが必要になることがあります。Sentinel はデータベースとイベントデータの格納にこの共有ストレージを使用します。予想されるイベント発生率およびデータ保持ポリシーに基づいて、共有ストレージのサイズが適切に設定されていることを確認します。

共有ストレージのセットアップの例

一般的な実装では、FibreChannel を使用してすべてのクラスタノードに接続された高速 SAN を使用し、ローカルイベントデータを保存するために大容量 RAID アレイを設置する場合があります。低速セカンダリストレージには、別の NAS ノードまたは iSCSI ノードを使用することもできます。クラスタノードがプライマリストレージを通常のプロックデバイスとしてマウントできるのであれば、この方法もソリューションに利用できます。セカンダリストレージもプロックデバイスとしてマウントできますが、NFS または CIFS ポリユームにすることも可能です。

注：NetIQ では、共有ストレージを構成し、クラスタノードごとにマウントをテストすることを推奨します。しかし、実際のストレージのマウントはクラスタ構成が処理します。

NetIQ では、次の手順で SUSE Linux VM がホスティングする iSCSI Target を作成することを推奨します：

- 1 storage03 (初期セットアップで作成した VM) に接続して、コンソールセッションを開始します。
- 2 次の dd コマンドを使用して、Sentinel プライマリストレージに必要なサイズのブランクファイルを作成します：

```
dd if=/dev/zero of=/localdata count=10240000 bs=1024
```
- 3 /dev/zero pseudo-device ファイルからコピーしてゼロを埋め込んだ 10GB のファイルを作成します。コマンドラインオプションの詳細については、dd コマンドの info または main ページを参照してください。

- 手順 1 ~ 3 を繰り返して、セカンダリストレージ用のファイルを作成します。

```
dd if=/dev/zero of=/networkdata count=10240000 bs=1024
```

注：この例では、サイズとパフォーマンス特性が同じ 2 つのディスクを表す、2 つのファイルを作成しました。運用展開では、プライマリストレージを高速な SAN 上に作成し、セカンダリストレージを低速な iSCSI、NFS、または CIFS ボリューム上に作成することができます。

30.2.1 iSCSI Target の環境設定

localdata ファイルと networkdata ファイルを iSCSI Target として設定します。

- コマンドラインから YaST を実行します (またはグラフィカルユーザインターフェースを使用することもできます) : /sbin/yast
- [**Network Devices (ネットワークデバイス)**] > [**Network Settings (ネットワーク設定)**] を選択します。
- [**概要**] タブが選択されていることを確認します。
- 表示されているリストからセカンダリ NIC を選択して、タブで [**編集**] に進み、Enter を押します。
- [**アドレス**] タブで、静的 IP アドレス 10.0.0.3 を割り当てます。これが内部 iSCSI 通信 IP になります。
- [**次**] をクリックし、[**OK**] をクリックします。
- メイン画面で、[**ネットワークサービス**]、[**iSCSI ターゲット**] の順に選択します。
- プロンプト画面が表示されたら、SUSE Linux 11 SP3 メディアから必要なソフトウェア (iscsitarget RPM) をインストールします。
- [**サービス**] をクリックして、[**When Booting(ブート時)**] オプションを選択して、オペレーティングシステムのブート時にサービスが開始するようにします。
- iSCSI 用の現行の OCF リソースエージェントが認証をサポートしていないため、[**Global(グローバル)**] をクリックしてから [**No Authentication(認証なし)**] を選択します。
- [**ターゲット**]、[**追加**] の順にクリックして、新規ターゲットを追加します。
iSCSI Target は ID を自動生成し、使用可能な LUN(ドライブ)の空のリストを表示します。
- [**追加**] をクリックして、新しい LUN を追加します。
- LUN 番号は 0 のままで、[**パス**] ダイアログ (Type=fileio の下) を参照して、作成した /localdata ファイルを選択します。ストレージ専用のディスクがある場合は、/dev/sdc などのブロックデバイスを指定します。
- 12 と 13 の手順を繰り返して、今回は LUN 1 と /networkdata を追加します。
- その他のオプションはデフォルトのままにしておきます。[**OK**] をクリックしてから [**次**] をクリックします。
- [**次**] をもう一度クリックしてデフォルト認証を選択してから、[**完了**] をクリックして設定を終了します。iSCSI の再起動を要求された場合は、それを受け入れます。
- YaST を終了します。

注：上記の手順を行うことにより、IP アドレス 10.0.0.3 のサーバに 2 つの iSCSI Target が公開されます。各クラスタノードで、ローカルデータ共有ストレージデバイスをマウントできることを確認してください。

30.2.2 iSCSI イニシエータの環境設定

次の手順で、デバイスのフォーマットを行います。

- 1 片方のクラスタノード (node1) に接続して、YaST を開始します。
- 2 [Network Devices (ネットワークデバイス)] > [Network Settings (ネットワーク設定)] を選択します。
- 3 [概要] タブが選択されていることを確認します。
- 4 表示されているリストからセカンダリ NIC を選択して、タブで [編集] に進み、Enter を押します。
- 5 [アドレス] をクリックして、静的 IP アドレス 10.0.0.1 を割り当てます。これが内部 iSCSI 通信 IP になります。
- 6 [次] を選択して、[OK] をクリックします。
- 7 [ネットワークサービス]、[iSCSI イニシエータ] の順にクリックします。
- 8 プロンプト画面が表示されたら、SUSE Linux 11 SP3 メディアから必要なソフトウェア (open-iscsi RPM) をインストールします。
- 9 [サービス] をクリックし、[When Booting(ブート時)] を選択して、ブート時に iSCSI サービスが開始するようにします。
- 10 [Discovered Targets(検出したターゲット)] をクリックして、[ディスクバリエーション] を選択します。
- 11 iSCSI Target の IP アドレス (10.0.0.3) を指定し、[No Authentication] を選択して、[次] をクリックします。
- 12 IP アドレスが 10.0.0.3 である検出された iSCSI Target を選択して、[ログイン] を選択します。
- 13 [Startup(起動)] ドロップダウンで自動的に切り替えて、[No Authentication(認証なし)] を選択してから、[次] をクリックします。
- 14 [Connected Targets(接続済みターゲット)] タブに切り替えて、ターゲットに接続していることを確認します。
- 15 環境設定を終了します。これで、iSCSI Target がクラスタノード上でブロックデバイスとしてマウントされました。
- 16 YaST メインメニューで、[システム]、[パーティショナ] の順に選択します。
- 17 [System View(システムビュー)] で、リストに新しいハードディスク (/dev/sdb や /dev/sdc など) が表示されます。これらは IET-VIRTUAL-DISK タイプになります。リストの先頭 (プライマリストレージのはずです) にタブを切り替えて、そのディスクを選択してから、Enter を押します。
- 18 [追加] を選択して、空のディスクに新規パーティションを追加します。ディスクをプライマリ ex3 パーティションとしてフォーマットし、マウントはしないでおきます。[Do not mount partition(パーティションをマウントしない)] オプションが選択されていることを確認します。

- 19 [次] を選択し、行われる変更内容を確認してから [完了] を選択します。この共有 iSCSI LUN に 1 つの大きなパーティションを作成することにした場合、最終的に /dev/sdb1 またはこれと同様のフォーマット済みディスク (以後 /dev/<SHARED1> と表記) が作成されているはずで
す。
- 20 パーティションに戻り、/dev/sdc またはセカンダリストレージに対応するブロックデバイスに
対して、パーティション作成 / フォーマットのプロセス (手順 16 ~ 19) を繰り返します。これ
により、/dev/sdc1 パーティションまたはこれと同様のフォーマット済みディスク (以後 /dev/
<NETWORK1> と表記) が作成されます。
- 21 YaST を終了します。
- 22 (条件による) 従来の HA インストールを実行している場合、マウントポイントを作成し、以下
のようにローカルパーティションのマウントをテストします (正確なデバイス名は、特定の実
装によって異なります)。
- ```
mkdir /var/opt/novell
mount /dev/<SHARED1> /var/opt/novell
```
- 新しいパーティション上でファイルを作成したり、パーティションがマウントされているファ  
イルを表示したりできるはずで  
す。
- 23 (条件による) 従来の HA インストールを実行している場合にアンマウントするには、以下を行  
います。
- ```
# umount /var/opt/novell
```
- 24 (条件による) HA アプライアンスのインストールの場合、手順 1 ~ 15 を繰り返して、各クラ
スタノードがローカル共有ストレージをマウントできるようにします。クラスタノードごと
に、手順 5 のノード IP を異なる IP に置き換えます。
- 25 (条件による) 従来の HA インストールの場合、手順 1 ~ 15、22、23 を繰り返して、各クラ
スタノードがローカル共有ストレージをマウントできるようにします。クラスタノードごと
に、手順 5 のノード IP を異なる IP に置き換えます。

30.3 Sentinel のインストール

Sentinel のインストールには 2 つのオプションがあります。1 つは、--location オプションを使用し
て、Sentinel のすべての部分を共有ストレージにインストールし、Sentinel インストール環境を共
有ストレージがマウントされた場所にリダイレクトさせる方法です。もう 1 つは、可変アプリケー
ションデータのみを共有ストレージにインストールする方法です。

NetIQ では、Sentinel をホスト可能な各クラスタノードにインストールすることを推奨します。
Sentinel を初めてインストールした後に、アプリケーションバイナリ、環境設定、およびすべての
データストアを含め、完全インストールを実行する必要があります。その他のクラスタノードへの
後続のインストールでは、アプリケーションのみをインストールします。共有ストレージをマウ
ントすると、Sentinel データが利用可能になります。

30.3.1 最初のノードインストール

- ◆ [155 ページの「従来の HA インストール」](#)
- ◆ [155 ページの「Sentinel HA アプライアンスのインストール」](#)

従来の HA インストール

- 1 いずれかのクラスタノード (node01) に接続して、コンソールウィンドウを開きます。
- 2 Sentinel インストーラ (tar.gz ファイル) をダウンロードして、そのクラスタノードの /tmp に保管します。
- 3 次のコマンドを実行します。

```
mount /dev/<SHARED1> /var/opt/novell
cd /tmp
tar -xvzf sentinel_server*.tar.gz
cd sentinel_server*
./install-sentinel --record-unattended=/tmp/install.props
```

- 4 標準インストールを最後まで実行し、Sentinel の環境設定を適切に行います。インストールプログラムによって、バイナリ、データベース、および環境設定の各ファイルがインストールされます。また、ログイン資格情報、環境設定、およびネットワークポートもセットアップされます。
- 5 Sentinel を起動して、基本機能をテストします。標準の外部クラスタノード IP を使用して Sentinel にアクセスできます。
- 6 次のコマンドを使用して、Sentinel をシャットダウンし、共有ストレージをマウント解除します。

```
rcsentinel stop
umount /var/opt/novell
```

これにより、自動起動スクリプトが削除され、クラスタは Sentinel を管理できるようになります。

```
cd /
insserv -r sentinel
```

Sentinel HA アプライアンスのインストール

Sentinel HA アプライアンスには、既にインストールされて環境設定されている Sentinel ソフトウェアが含まれています。HA 用に Sentinel ソフトウェアを環境設定するには、以下のステップを実行します。

- 1 いずれかのクラスタノード (node01) に接続して、コンソールウィンドウを開きます。
- 2 以下のディレクトリを選択します。

```
cd /opt/novell/sentinel/setup
```

- 3 環境設定を記録します。
 - 3a 次のコマンドを実行します：

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

このステップでは、install.props ファイルに環境設定を記録します。このファイルは、install-resources.sh スクリプトを使用してクラスタリソースを環境設定するのに必要です。

- 3b オプションを指定して、Sentinel 設定タイプを選択します。

3c 2 を指定して、新しいパスワードを入力します。

1 を指定すると、install.props ファイルにパスワードは保管されません。

4 以下のコマンドを使用して、Sentinel をシャットダウンします。

```
rksentinel stop
```

これにより、自動起動スクリプトが削除され、クラスタは Sentinel を管理できるようになります。

```
insserv -r sentinel
```

5 以下のコマンドを使用して、Sentinel データフォルダを共有ストレージに移動します。この移動により、ノードは共有ストレージを介して Sentinel データフォルダを利用できます。

```
mkdir -p /tmp/new
```

```
mount /dev/<SHARED1> /tmp/new
```

```
mv /var/opt/novell/sentinel /tmp/new
```

```
umount /tmp/new/
```

6 以下のコマンドを使用して、共有ストレージへの Sentinel データフォルダの移動を検証します。

```
mount /dev/<SHARED1> /var/opt/novell/
```

```
umount /var/opt/novell/
```

30.3.2 後続のノードインストール

- ◆ [156 ページの「従来の HA インストール」](#)
- ◆ [157 ページの「Sentinel HA アプライアンスのインストール」](#)

その他のノードでインストールを繰り返します：

最初の Sentinel インストーラは Sentinel 自体が使用するユーザアカウントを作成します。そして、インストール時点から次に使用可能なユーザ ID を使用します。後続のインストールを無人モードで実行すると、アカウント作成時に使用したのと同じユーザ ID を使用しようとしてますが、(クラスタノードがインストール時のノードと同じでない場合には)競合が発生する可能性があります。以下のいずれかを行うことを強くお勧めします。

- ◆ クラスタノード全体でユーザアカウントデータベースを(手動でLDAPからまたは同様の方法で)同期して、後続のインストールを実行する前に同期を完了させておきます。この場合、インストーラはユーザアカウントの存在を検出して、既存のアカウントを使用します。
- ◆ 後続の無人インストールの出力を確認します。同じユーザ ID でユーザアカウントを作成できなかった場合、警告が出されます。

従来の HA インストール

- 1 各追加クラスタノード (node02) に接続して、コンソールウィンドウを開きます。
- 2 次のコマンドを実行します。

```
cd /tmp
```

```
scp root@node01:/tmp/sentinel_server*.tar.gz .
```

```
scp root@node01:/tmp/install.props .
tar -xvzf sentinel_server*.tar.gz
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
insserv -r sentinel
```

Sentinel HA アプライアンスのインストール

- 1 各追加クラスタノード (node02) に接続して、コンソールウィンドウを開きます。
- 2 次のコマンドを実行します：

```
insserv -r sentinel
```

- 3 Sentinel サービスを停止します。

```
rcsentinel stop
```

- 4 Sentinel ディレクトリを削除します。

```
rm -rf /var/opt/novell/sentinel
```

この処理が終わると、Sentinel がすべてのノードにインストールされているはずですが、各種キーが同期されるまで、最初のノード以外のノードでは Sentinel が正常に動作しない可能性があります。これは、クラスタリソースを設定した場合に発生します。

30.4 クラスタインストール

クラスタソフトウェアは、従来の高可用性 (HA) インストール環境にのみインストールする必要があります。Sentinel HA アプライアンスにはクラスタソフトウェアが含まれており、手動でのインストールは必要ありません。

NetIQ は、次の手順で、SUSE Linux High Availability Extension に Sentinel 固有のリソースエージェントオーバーレイを指定して設定することを推奨します。

- 1 各ノードにクラスタソフトウェアをインストールします。
- 2 各ノードクラスタをクラスタマネージャに登録します。
- 3 クラスタ管理コンソールに各クラスタノードが表示されることを確認します。

注： Sentinel 用の OCF リソースエージェントはシンプルなシェルスクリプトで、さまざまな検査を実行して Sentinel が機能しているかどうかを検証します。Sentinel の監視に OCF リソースエージェントを使用しない場合は、ローカルクラスタ環境を監視する同様のソリューションを開発する必要があります。独自に開発する場合は、Sentinel ダウンロードパッケージの Sentinelha.rpm ファイルに格納されている既存のリソースエージェントを確認してください。

- 4 [SLE HAE 資料に従って、コアとなる SLE HAE ソフトウェアをインストールします。](#) SLES アドオンのインストールについては、『[Deployment Guide](#)』を参照してください。
- 5 すべてのクラスタノードに対してステップ 4 を繰り返します。このアドオンをインストールすると、コアとなるクラスタ管理および通信ソフトウェアだけでなく、クラスタリソースの監視に使用される多数のリソースエージェントもインストールされます。

- さらに RPM をインストールして、Sentinel 固有のクラスタリソースエージェントを追加します。この HA RPM は、Sentinel をインストールする際に解凍したデフォルトの Sentinel ダウンロードに保存されている、`novell-Sentinelha-<Sentinel_version>*.rpm` に含まれています。
- 各クラスタノードで、`novell-Sentinelha-<Sentinel_version>*.rpm` ファイルを `/tmp` ディレクトリにコピーしてから、次のコマンドを実行します。

```
cd /tmp
```

```
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

30.5 クラスタ環境設定

クラスタソフトウェアを設定して、各クラスタノードをクラスタのメンバーとして登録する必要があります。この環境設定の一環として、クラスタの整合性を確保するために、フェンシングと Shoot The Other Node In The Head (STONITH) リソースを設定することもできます。

NetIQ では、次の手順でクラスタの環境設定を行うことを推奨します。

このソリューションでは、内部クラスタ通信にプライベート IP アドレスを使用し、ネットワーク管理者に対するマルチキャストアドレスの要求が最小限で済むようにユニキャストを使用する必要があります。また、共有ストレージをホストしているのと同じ SUSE Linux VM で、iSCSI Target をフェンシングのための SBD デバイスとして機能するように設定して使用する必要もあります。

SBD のセットアップ

- `storage03` に接続して、コンソールセッションを開始します。次の `dd` コマンドを使用して、希望する任意のサイズのブランクファイルを作成します：

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```
- ゼロを埋め込んだ 1MB のファイルを `/dev/zero pseudo-device` からコピーして作成します。
- コマンドラインまたはグラフィカルユーザインタフェースから YaST を実行します：`/sbin/yast`
- [ネットワークサービス]、[iSCSI ターゲット] の順に選択します。
- [ターゲット] をクリックして、既存のターゲットを選択します。
- [編集] を選択します。UI に使用可能な LUN(ドライブ) のリストが表示されます。
- [追加] を選択して、新しい LUN を追加します。
- LUN 番号は 2 のままにしておきます。[パス] ダイアログを参照して、作成した `/sbd` ファイルを選択します。
- その他のオプションはデフォルトのままにしておき、[OK] を選択してから [次] を選択し、もう一度 [次] をクリックしてデフォルト認証オプションを選択します。
- [完了] をクリックして、設定を終了します。必要に応じてサービスを再起動します。YaST を終了します。

注：以下のステップでは、各クラスタノードが他のすべてのクラスタノードのホスト名を解決できなければなりません(それができないと、ファイル同期サービス `csync2` が失敗します)。DNS がセットアップされていないまたは使用できない場合は、各ホストのエントリを `/etc/hosts` ファイルに追加します。このファイルには各 IP とそのホスト名 (`hostname` コマンドを実行して返されるようなリスト) がリストされています。また、ループバック IP アドレスにホスト名を割り当てることのないようにします。

次の手順を行うことにより、IP アドレス 10.0.0.3 (storage03) のサーバの SBD デバイスの iSCSI Target が公開されます。

ノードの設定

クラスタノード (node01) に接続して、コンソールを開きます：

- 1 YaST を実行します。
- 2 [ネットワークサービス]、[iSCSI イニシエータ] の順に開きます。
- 3 [Connected Targets(接続済みターゲット)] を選択してから、上記の手順で設定した iSCSI Target を選択します。
- 4 [ログアウト] オプションを選択して、Target をログアウトします。
- 5 [Discovered Targets(検出したターゲット)] タブに切り替えて、[Target(ターゲット)] を選択し、もう一度ログインし直して、デバイスのリストを更新します (自動起動オプションと [No Authentication(認証なし)] はそのままにしておきます)。
- 6 [OK] を選択して、iSCSI イニシエータツールを終了します。
- 7 [システム]、[Partitioner(パーティショナ)] の順に開いて、SBD デバイスを 1MB IET-VIRTUAL-DISK として特定します。このデバイスは /dev/sdd または同様の形式でリストされます。どちらかを確認します。
- 8 YaST を終了します。
- 9 コマンド `ls -l /dev/disk/by-id/` を実行して、上記の手順で特定したデバイス名にリンクされているデバイス ID を確認します。
- 10 コマンド `sleha-init` を実行します。
- 11 バインド先のネットワークアドレスの入力を要求されたら、外部 NIC IP (172.16.0.1) を指定します。
- 12 デフォルトのマルチキャストアドレスおよびポートを受け入れます。この設定は後で上書きします。
- 13 SBD の有効化に「y」と入力してから、`/dev/disk/by-id/<device id>` を指定します。<device id> は上記の手順で特定した ID です (Tab キーを使ってパスを自動補完することができます)。
- 14 ウィザードを最後まで進めて、エラーの報告がないことを確認します。
- 15 YaST を起動します。
- 16 [High Availability(高可用性)]、[Cluster(クラスタ)] の順に選択します (一部のシステムでは [Cluster(クラスタ)] を選択するだけです)。
- 17 左のボックスで、[Communication Channels(通信チャネル)] が選択されていることを確認します。
- 18 設定の最上部行に移動し、udp の選択を **udpu** に変更します (これで、マルチキャストを無効にし、ユニキャストを選択します)。
- 19 [Add a Member Address(メンバアドレスを追加)] を選択して、このノード (172.16.0.1) を指定してから、この手順を繰り返して他のクラスタノード (172.16.0.2) を追加します。
- 20 [完了] をクリックして設定を完了します。
- 21 YaST を終了します。
- 22 コマンドの `/etc/rc.d/openais restart` を実行して、新しい同期プロトコルでクラスタサービスを再起動します。

各追加クラスタノード (node02) に接続して、コンソールを開きます：

- 1 YaST を実行します。
- 2 [ネットワークサービス]、[iSCSI イニシエータ] の順に開きます。
- 3 [Connected Targets(接続済みターゲット)] を選択してから、上記の手順で設定した iSCSI Target を選択します。
- 4 [ログアウト] オプションを選択して、Target をログアウトします。
- 5 [Discovered Targets(検出したターゲット)] タブに切り替えて、[Target(ターゲット)] を選択し、もう一度ログインし直して、デバイスのリストを更新します (自動起動オプションと [No Authentication(認証なし)] はそのままにしておきます)。
- 6 [OK] を選択して、iSCSI イニシエータツールを終了します。
- 7 次のコマンドを実行します：sleha-join
- 8 最初のクラスタノードの IP アドレスを入力します。

(条件による) クラスタが正常に起動しない場合は、次の手順を実行します。

- 1 /etc/corosync/corosync.conf を node01 から node02 に手でコピーするか、node01 で csync2 -x -v を実行する、または YaST を使用して node02 上にクラスタを手動で設定します。
- 2 node02 で /etc/rc.d/openais start を実行します。

(条件による) xinetd サービスが新しい csync2 サービスを正しく追加しないと、スクリプトは正常に機能しません。もう一方のノードがクラスタ設定ファイルをこのノードに同期できるようにするためには、xinetd サービスが必須です。csync2 run failed のようなエラーが表示されるときは、この問題である可能性があります。

この問題を解決するには、kill -HUP `cat /var/run/xinetd.init.pid` コマンドを実行してから、sleha-join スクリプトを再実行します。

- 3 各クラスタノードで crm_mon を実行して、クラスタが正常に稼働しているかどうかを確認します。「hawk」という Web コンソールを使用して、クラスタを確認することもできます。デフォルトのログイン名は hacluster で、パスワードは linux です。

(条件による) 環境に応じて、次のタスクを実行してさらにパラメータを変更します。

- 1 2 ノードクラスタの環境で起きた 1 つのノードの障害がクラスタ全体を予期せず停止させないように、グローバルクラスタオプション no-quorum-policy を ignore に設定します。

```
crm configure property no-quorum-policy=ignore
```

注：クラスタに 3 つ以上のノードがある場合は、このオプションを設定しないでください。

- 2 所定の場所でのリソースの実行およびリソースの移動がリソースマネージャで許可されるようにするには、グローバルクラスタオプション default-resource-stickiness を「1」に設定します。

```
crm configure property default-resource-stickiness=1
```

30.6 リソースの環境設定

リソースエージェントはデフォルトで SLE HAE に付属しています。SLE HAE を使用しない場合は、代替テクノロジーを使用して以下の追加リソースを監視する必要があります。

- ◆ このソフトウェアが使用する共有ストレージに相当するファイルシステムリソース。

- ◆ サービスへのアクセスに使用する仮想 IP に相当する IP アドレスリソース。
- ◆ 環境設定とイベントメタデータを保存する PostgreSQL データベースソフトウェア。

NetIQ では、次の方法でリソースの環境設定を行うことを推奨します。

NetIQ は、クラスタ環境設定の補助のために、crm スクリプトを提供しています。このスクリプトは、Sentinel インストールの途中で生成される無人セットアップファイルから必要な設定変数を取り出します。セットアップファイルを生成していない場合、またはリソースの環境設定を変更する場合は、それぞれに応じて次の手順でスクリプトを編集できます。

- 1 Sentinel をインストールした元のノードに接続します。

注: このノードは、Sentinel の完全インストールを実行したノードである必要があります。

- 2 スクリプトの内容を次のように編集します。<SHARED1> は以前に作成した共有ボリュームです。

```
mount /dev/<SHARED1> /var/opt/novell
cd /usr/lib/ocf/resource.d/novell
./install-resources.sh
```

- 3 (条件による) クラスタ内で新規リソースに関する問題が発生する可能性もあります。その場合は、node02 上で /etc/rc.d/openais restart を実行します。
- 4 install-resources.sh スクリプトは、2 つの値、すなわち一般ユーザが Sentinel にアクセスするときに使用する仮想 IP および共有ストレージのデバイス名の入力を要求し、その後必要なクラスタリソースを自動生成します。スクリプトに指定する共有ボリュームは既にマウント済みのものでなければならないこと、および Sentinel インストール時に作成された無人インストールファイル (/tmp/install.props) も必要であることに注意してください。このスクリプトは最初にインストールを実行したノードのみで実行すればよく、必要なすべての設定ファイルは他のノードに自動的に同期されます。
- 5 ご使用の環境がこの NetIQ 推奨ソリューションとは異なる場合は、同一ディレクトリにある resources.cli ファイルを編集し、その中のプリミティブ型定義を変更してください。たとえば、推奨ソリューションではシンプルなファイルシステムリソースを使用していますが、もっとクラスタ指向の cLVM リソースを使用する場合もあります。
- 6 シェルスクリプトを実行した後、crm status コマンドを実行することができます。出力は次のように表示されます。

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

```
Online: [ node01, node02 ]
stonith-sbd (stonith:external/sbd): Started node01
Resource Group: sentinelgrp
sentinelip (ocf::heartbeat:IPaddr2): Started node01
sentinelifs (ocf::heartbeat:Filesystem): Started node01
sentinelldb (ocf::novell:pgsql): Started node01
sentinelserver (ocf::novell:sentinel): Started node01
```

- 7 この時点で、関係する Sentinel リソースがクラスタに設定されています。クラスタ管理ツールで `crm status` を実行するなどして、リソースがどのように設定およびグループ化されているかを確認できます。

30.7 セカンダリストレージ設定

Sentinel がイベントパーティションをより安価なストレージに移動できるようにセカンダリストレージを環境設定するには、次の手順を実行します。

注：この手順はオプションであり、システムの他のストレージを設定したのと同じようにセカンダリストレージを高可用性にする必要はありません。SAN、非 SAN、NFS、または CIFS ボリュームからマウントされている任意のディレクトリを使用できます。

- 1 Sentinel Web コンソールのトップメニューバーで、[ストレージ] をクリックします。
- 2 [環境設定] を選択します。
- 3 未設定のセカンダリストレージのラジオボタンを 1 つ選択します。

NetIQ では、シンプルな iSCSI Target をネットワーク共有ストレージの場所として使用することを推奨します。設定はプライマリストレージとほぼ同じです。運用環境では、ストレージテクノロジーが異なる場合があります。

以下の手順に従って、Sentinel が使用するセカンダリストレージを設定します。

注：NetIQ ではこのソリューションに iSCSI Target を使用することを推奨しているため、ターゲットはセカンダリストレージとして使用されるディレクトリとしてマウントされます。プライマリストレージのファイルシステムを環境設定したような方法で、マウントをファイルシステムリソースとして環境設定する必要があります。異なる設定が指定される可能性もあるため、この設定がリソースインストールスクリプトの一部として自動で設定されることはありません。

- 1 上記のステップを確認して、セカンダリストレージ用にどのパーティションが作成されたかを判別します (`/dev/<NETWORK1>`、または `/dev/sdc1` など)。必要であれば、パーティションをマウントできる空のディレクトリを作成します (`/var/opt/netdata` など)。
- 2 ネットワークファイルシステムをクラスタリソースとしてセットアップします。Web コンソールを使用するかまたは次のコマンドを実行します：

```
crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
```

ここで、`/dev/<NETWORK1>` は前述の「共有ストレージのセットアップ」セクションで作成したパーティションで、`<PATH>` はストレージをマウントする任意のローカルディレクトリです。

- 3 管理対象リソースのグループに新規リソースを追加します：

```
crm resource stop sentinelgrp
crm configure delete sentinelgrp
crm configure group sentinelgrp sentinelip sentinelifs sentinelnetfs sentineldb
sentinelserver
crm resource start sentinelgrp
```

- 4 現在リソースをホストしているノードに接続して (crm status または Hawk を使用)、ネットワークストレージが正しくマウントされていることを確認します (mount コマンドを使用)。
- 5 Sentinel Web インタフェースにログインします。
- 6 [ストレージ] を選択してから [環境設定] を選択し、未設定のセカンダリストレージの [SAN (ローカルにマウント)] を選択します。
- 7 セカンダリストレージがマウントされているパスを、たとえば /var/opt/netdata のように入力します。

NetIQ では、シンプルなファイルシステムリソースエージェントなど、必要なリソースには単純なものを使用することを推奨しています。お客様のご希望によっては、cLVM (論理ボリューム対応のファイルシステム) のような、より高性能なクラスタリソースを使用することも可能です。

31 高可用性の Sentinel のアップグレード

HA 環境で Sentinel をアップグレードする場合は、まず、クラスタ内のパッシブノードをアップグレードしてから、アクティブクラスタノードをアップグレードする必要があります。

- ◆ [165 ページのセクション 31.1 「前提条件」](#)
- ◆ [165 ページのセクション 31.2 「従来の Sentinel HA インストールのアップグレード」](#)
- ◆ [167 ページのセクション 31.3 「Sentinel HA アプライアンスインストールのアップグレード」](#)

31.1 前提条件

- ◆ [NetIQ ダウンロード Web サイト](#)から最新のインストーラをダウンロードします。
- ◆ SLES オペレーティングシステム (カーネルバージョン 3.0.101 以降) を使用している場合、コンピュータにウォッチドッグドライバを手動でロードする必要があります。ご使用のコンピュータハードウェア用の適切なウォッチドッグドライバを見つけるには、ハードウェアベンダーに連絡してください。ウォッチドッグドライバをロードするには、以下を実行します。

1. コマンドプロンプトで、以下のコマンドを実行し、現在のセッションでウォッチドッグドライバをロードします。

```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```

2. 以下の行を `/etc/init.d/boot.local` ファイルに追加し、コンピュータが各ブート時にウォッチドッグドライバを自動的にロードするようにします。

```
/sbin/modprobe -v --ignore-install <watchdog driver name>
```

31.2 従来の Sentinel HA インストールのアップグレード

- 1 クラスタの保守モードを有効にします。

```
crm configure property maintenance-mode=true
```

保守モードは、Sentinel をアップデートする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。このコマンドは、どのクラスタノードからでも実行することができます。

- 2 保守モードがアクティブかどうか確認します。

```
crm status
```

クラスタリソースは非管理状態と表示されるはずです。

- 3 パッシブクラスタノードをアップデートします。

- 3a クラスタスタックを停止します。

```
rcopenais stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

3b Sentinel をアップグレードするサーバに `root` としてログインします。

3c `tar` ファイルからインストールファイルを抽出します。

```
tar xfz <install_filename>
```

3d インストールファイルを抽出したディレクトリで、次のコマンドを実行します。

```
./install-sentinel --cluster-node
```

3e アップグレード完了後、クラスタスタックを再起動します。

```
rcopenais start
```

すべてのパッシブクラスタノードに対してステップ 3 を繰り返します。

3f 自動起動スクリプトを削除して、クラスタが製品を管理できるようにします。

```
cd /
```

```
insserv -r sentinel
```

4 アクティブなクラスタノードをアップグレードします。

4a 環境設定をバックアップしてから、ESM エクスポートを作成します。

データのバックアップの詳細については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。

4b クラスタスタックを停止します。

```
rcopenais stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

4c Sentinel をアップグレードするサーバに `root` としてログインします。

4d 次のコマンドを実行して、`tar` ファイルからインストールファイルを抽出します。

```
tar xfz <install_filename>
```

4e インストールファイルを抽出したディレクトリで、次のコマンドを実行します。

```
./install-sentinel
```

4f アップグレード完了後、クラスタスタックを起動します。

```
rcopenais start
```

4g 自動起動スクリプトを削除して、クラスタが製品を管理できるようにします。

```
cd /
```

```
insserv -r sentinel
```

4h 次のコマンドを実行して、環境設定ファイルの変更を同期します。

```
run csync2 -x -v
```

5 クラスタの保守モードを無効にします。

```
crm configure property maintenance-mode=false
```

このコマンドは、どのクラスタノードからでも実行することができます。

6 保守モードがアクティブではないことを確認します。

```
crm status
```

クラスタリソースは起動済みと表示されるはずですが。

7 (任意) Sentinel のアップグレードが成功したかどうか確認します。

```
rcsentinel version
```

31.3 Sentinel HA アプライアンスインストールのアップグレード

Zypper パッチや WebYast を使用して、Sentinel HA アプライアンスインストールをアップグレードできます。

- ◆ [167 ページのセクション 31.3.1「Zypper を使用した Sentinel HA アプライアンスのアップグレード」](#)
- ◆ [169 ページのセクション 31.3.2「WebYast を使用した Sentinel HA アプライアンスのアップグレード」](#)

31.3.1 Zypper を使用した Sentinel HA アプライアンスのアップグレード

アップグレードの前に、WebYast ですべてのアプライアンスノードを登録する必要があります。詳細については、[85 ページのセクション 13.3.3「アップデートの登録」](#)を参照してください。アプライアンスを登録しないと、Sentinel で黄色の警告が表示されます。

1 クラスタの保守モードを有効にします。

```
crm configure property maintenance-mode=true
```

保守モードは、Sentinel ソフトウェアをアップデートする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。このコマンドは、どのクラスタノードからでも実行することができます。

2 保守モードがアクティブかどうか確認します。

```
crm status
```

クラスタリソースは非管理状態と表示されるはずですが。

3 パッシブクラスタノードをアップデートします。

3a Sentinel HA アプライアンスの更新をダウンロードします。

```
zypper -v patch -d
```

このコマンドは、Sentinel を含むアプライアンスにインストールされたパッケージの更新を `/var/cache/zypp/packages` にダウンロードします。

3b クラスタスタックを停止します。

```
rcopenais stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

3c 更新をダウンロードしたら、以下のコマンドを使用して、更新をインストールします。

```
rpm -Uvh /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/rpm/
noarch/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-Updates/
rpm/x86_64/*.rpm /var/cache/zypp/packages/sentinel_server_7000_x86_64-
Updates/rpm/i586/*.rpm --excludepath=/var/opt/novell/
```

3d 以下のスクリプトを実行して、アップグレードプロセスを完了します。

```
/var/adm/update-scripts/sentinel_server_ha_x86_64-update-<version>-
overlay_files.sh
```

3e アップグレード完了後、クラスタスタックを再起動します。

```
rcopenais start
```

すべてのパッシブクラスタノードに対してステップ 3 を繰り返します。

4 アクティブなクラスタノードをアップグレードします。

4a 環境設定をバックアップしてから、ESM エクスポートを作成します。

データのバックアップ方法については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。

4b クラスタスタックを停止します。

```
rcopenais stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

4c 管理者として Sentinel アプライアンスにログインします。

4d Sentinel アプライアンスをアップグレードする場合は、[アプライアンス] をクリックして WebYaST を起動します。

4e アップデートがあるかどうかを確認するには、[更新] をクリックします。

4f 更新を選択して適用します。

更新が完了するまで数分かかる場合があります。更新が成功すると、WebYaST のログインページが表示されます。

アプライアンスをアップグレードする前に、WebYaST は Sentinel サービスを自動的に停止します。アップグレードが完了した後で、このサービスを手動で再開する必要があります。

4g Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

4h アップグレード完了後、クラスタスタックを再起動します。

```
rcopenais start
```

4i 次のコマンドを実行して、環境設定ファイルの変更を同期します。

```
run csync2 -x -v
```

5 クラスタの保守モードを無効にします。

```
crm configure property maintenance-mode=false
```

このコマンドは、どのクラスタノードからでも実行することができます。

6 保守モードがアクティブではないことを確認します。

```
crm status
```

クラスタリソースは起動済みと表示されるはずですが。

7 (任意) Sentinel のアップグレードが成功したかどうか確認します。

```
rcsentinel version
```

31.3.2 WebYast を使用した Sentinel HA アプライアンスのアップグレード

アップグレードの前に、WebYast ですべてのアプライアンスノードを登録する必要があります。詳細については、[85 ページのセクション 13.3.3 「アップデートの登録」](#) を参照してください。アプライアンスを登録しないと、Sentinel で黄色の警告が表示されます。

1 クラスタの保守モードを有効にします。

```
crm configure property maintenance-mode=true
```

保守モードは、Sentinel ソフトウェアをアップデートする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。このコマンドは、どのクラスタノードからでも実行することができます。

2 保守モードがアクティブかどうか確認します。

```
crm status
```

クラスタリソースは非管理状態と表示されるはずですが。

3 パッシブクラスタノードをアップデートします。

3a クラスタスタックを停止します。

```
rcopenais stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

3b パッシブクラスタノードの URL をポート 4984 を使用して指定し (https://<IP_address>:4984)、WebYaST を起動します。<IP_address> はパッシブクラスタノードの IP アドレスです。管理者として Sentinel アプライアンスにログインします。

3c アップデートがあるかどうかを確認するには、[更新] をクリックします。

3d 更新を選択して適用します。

更新が完了するまで数分かかる場合があります。更新が成功すると、WebYaST のログインページが表示されます。

3e アップグレード完了後、クラスタスタックを再起動します。

```
rcopenais start
```

すべてのパッシブクラスタノードに対して [ステップ 4](#) を繰り返します。

4 アクティブなクラスタノードをアップグレードします。

4a 環境設定をバックアップしてから、ESM エクスポートを作成します。

データのバックアップ方法については、『[NetIQ Sentinel Administration Guide](#)』の「[Backing Up and Restoring Data](#)」を参照してください。

4b クラスタスタックを停止します。

```
rcopenais stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

4c 管理者として Sentinel アプライアンスにログインします。

4d Sentinel アプライアンスをアップグレードする場合は、[**アプライアンス**] をクリックして WebYaST を起動します。

4e アップデートがあるかどうかを確認するには、[**更新**] をクリックします。

4f 更新を選択して適用します。

更新が完了するまで数分かかる場合があります。更新が成功すると、WebYaST のログインページが表示されます。

アプライアンスをアップグレードする前に、WebYaST は Sentinel サービスを自動的に停止します。アップグレードが完了した後で、このサービスを手動で再開する必要があります。

4g Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

4h アップグレード完了後、クラスタスタックを再起動します。

```
rcopenais start
```

4i 次のコマンドを実行して、環境設定ファイルの変更を同期します。

```
run csync2 -x -v
```

5 クラスタの保守モードを無効にします。

```
crm configure property maintenance-mode=false
```

このコマンドは、どのクラスタノードからでも実行することができます。

6 保守モードがアクティブではないことを確認します。

```
crm status
```

クラスタリソースは起動済みと表示されるはずです。

7 (任意) Sentinel のアップグレードが成功したかどうか確認します。

```
rcsentinel version
```

32 バックアップと復元

本マニュアルに記述されている高可用性フェールオーバークラスタは一定レベルの冗長性を提供するので、クラスタ内のあるノードでサービスに障害が起きた場合でも、自動的にフェールオーバーして、クラスタ内の別のノード上に復元します。このようなイベントが生じたとき、障害が発生したノードを運用状態に戻して、システムの冗長性を回復し、再び障害が発生したときにシステムを保護できるようにすることが重要です。このセクションでは、さまざまなエラー条件で障害が発生したノードを復元する方法について説明します。

- ◆ [171 ページのセクション 32.1「バックアップ」](#)
- ◆ [171 ページのセクション 32.2「回復」](#)

32.1 バックアップ

本マニュアルに記述されているような高可用性フェールオーバークラスタは一定レベルの冗長性を提供していますが、環境設定やデータについては従来の方法でバックアップを定期的にとっておくことは重要です。これらは、一度失われたり壊れたりしても簡単には回復できない場合が多いからです。『*NetIQ Sentinel Administration Guide*』のセクション「[「Backing Up and Restoring Data」](#)」では、Sentinel の組み込みツールを使用してバックアップを作成する方法が説明されています。クラスタ内のパッシブノードは共有ストレージデバイスに対する必要なアクセス権を持っていないため、これらのツールはクラスタ内のアクティブノードで使用します。他のバックアップツール製品を代わりに使用することもできますが、どのノードで使用できるかに関して異なる要件を持っている可能性があります。

32.2 回復

- ◆ [171 ページのセクション 32.2.1「一時的な障害」](#)
- ◆ [171 ページのセクション 32.2.2「ノードの破損」](#)
- ◆ [172 ページのセクション 32.2.3「クラスタデータの設定」](#)

32.2.1 一時的な障害

障害が一時的であり、アプリケーション、オペレーティングシステムソフトウェア、および環境設定に明らかな破損がない場合は、ノードをリブートするなどして一時的な障害を解除するだけでノードを運用状態に復元できます。必要であれば、クラスタ管理ユーザインタフェースを使用して、実行中のサービスをフェールバックして元のクラスタノードに戻すことができます。

32.2.2 ノードの破損

障害によって、ノードのストレージシステム上にあるアプリケーション、オペレーティングシステムソフトウェア、または環境設定に破損が生じた場合は、破損したソフトウェアを再インストールする必要があります。本マニュアルで既に説明したクラスタのノードを追加するステップを繰り返すことで、ノードを運用状態に復元することができます。必要であれば、クラスタ管理ユーザインタフェースを使用して、実行中のサービスをフェールバックして元のクラスタノードに戻すことができます。

32.2.3 クラスタデータの設定

共有ストレージデバイス上でデータの破損が生じて共有ストレージデバイスが回復不能である場合は、その影響がクラスタ全体に及んでおり、本マニュアルで説明されている高可用性フェールオーバークラスタを使用しても自動的に回復できない状態になっていると考えられます。『[NetIQ Sentinel Administration Guide](#)』のセクション「[Backing Up and Restoring Data](#)」では、Sentinelに組み込まれているツールを使用してバックアップから復元する方法が説明されています。クラスタ内のパッシブノードは共有ストレージデバイスに対する必要なアクセス権を持っていないため、これらのツールはクラスタ内のアクティブノードで使用します。他のバックアップ復元ツール製品を代わりに使用することもできますが、どのノードで使用できるかに関して異なる要件を持っている可能性があります。

VII 付録

- ◆ 175 ページの付録 A「トラブルシューティング」
- ◆ 177 ページの付録 B「アンインストール中」

A トラブルシューティング

このセクションでは、インストール時に発生する可能性があるいくつかの問題とその解決方法について説明します。

A.1 ネットワーク接続が不正なためにインストールが失敗する

最初のブート時に、インストーラでネットワーク設定が不正であることを検出すると、エラーメッセージが表示されます。ネットワークが使用できない場合、アプライアンスへの Sentinel のインストールは失敗します。

この問題を解決するには、ネットワークを正しく設定します。環境設定を確認するには、有効な IP アドレスを返す `ipconfig` コマンドと、有効なホスト名を返す `hostname -f` コマンドを使用します。

A.2 イメージを作成したコレクタマネージャまたは関連エンジンの UUID が作成されない

コレクタマネージャサーバのイメージを作成し (たとえば、ZENworks イメージングを使用)、別のマシンにそのイメージを復元する場合、Sentinel はコレクタマネージャの新しいインスタンスを一意的に識別しません。これは、UUID が重複しているために発生します。

新しくインストールしたコレクタマネージャのシステムで次の手順を実行し、新しい UUID を生成する必要があります。

- 1 /var/opt/novell/sentinel/data フォルダにある `host.id` または `sentinel.id` ファイルを削除します。
- 2 コレクタマネージャを再起動します。
コレクタマネージャが自動的に UUID を生成します。

A.3 ログイン後に Internet Explorer で Web インタフェースがブランクになる

インターネットの [セキュリティのレベル] が [高] に設定されている場合、Sentinel にログインしても、ファイルダウンロードのポップアップがブラウザによってブロックされることがあります。この問題を回避するには、次のようにしてセキュリティのレベルをいったん [中高] に設定した後、[カスタム] レベルに変更してください。

1. [ツール] > [インターネットオプション] > [セキュリティ] の順にクリックし、セキュリティのレベルを [中高] に設定します。

2. [ツール] > [互換表示] オプションが選択されていないことを確認します。
3. [ツール] > [インターネットオプション] > [セキュリティ] タブ > [レベルのカスタマイズ] の順にクリックし、[ダウンロード] セクションまで下にスクロールし、[ファイルのダウンロード時に自動的にダイアログを表示] オプションの [有効にする] を選択します。

B アンインストール中

この付録では、Sentinel のアンインストールおよびアンインストール後の作業について説明します。

- ◆ 177 ページのセクション B.1 「アンインストールのためのチェックリスト」
- ◆ 177 ページのセクション B.2 「Sentinel のアンインストール」
- ◆ 179 ページのセクション B.3 「アンインストール後の作業」

B.1 アンインストールのためのチェックリスト

以下のチェックリストを使用して、Sentinel をアンインストールします。

- Sentinel サーバをアンインストールする。
- コレクタマネージャおよび関連エンジンをアンインストールする(インストールされている場合)。
- アンインストール後の作業を実行して、Sentinel のアンインストールを完了する。

B.2 Sentinel のアンインストール

Sentinel のインストールを削除するのに便利なアンインストーラスクリプトを使用できます。新規のインストールを実行する前に、以前のインストールのファイルまたはシステム設定が残らないようにするために、次の手順をすべて実行する必要があります。

警告: これらの手順では、オペレーティングシステムの設定やファイルを変更します。システム設定やファイルの変更方法に精通したユーザでない場合は、システム管理者に問い合わせてください。

B.2.1 Sentinel サーバのアンインストール

次の手順に従って、Sentinel サーバをアンインストールします。

- 1 Sentinel サーバに root としてログインします。

注: root ユーザとしてインストールを実行している場合、root 以外のユーザで Sentinel サーバをアンインストールすることはできません。ただし、root 以外のユーザがインストールした場合は、root 以外のユーザで Sentinel サーバをアンインストールできます。

- 2 次のディレクトリにアクセスします。

```
/opt/novell/sentinel/setup/
```

- 3 次のコマンドを実行します。

```
./uninstall-sentinel
```

- 4 アンインストールを続行するかどうか再確認を求められたら、「y」を押します。
スクリプトはまずサービスを停止し、その後に削除を実行します。

B.2.2 コレクタマネージャおよび関連エンジンのアンインストール

次の手順に従って、コレクタマネージャおよび関連エンジンをアンインストールします：

- 1 rootとしてコレクタマネージャおよび関連エンジンのコンピュータにログインします。

注： root ユーザとしてインストールを実行した場合、root 以外のユーザとしてリモートコレクタマネージャまたはリモート関連エンジンをアンインストールすることはできません。ただし、root 以外のユーザとしてインストールを行った場合は、root 以外のユーザでアンインストールできます。

- 2 次の場所に移動します。

```
/opt/novell/sentinel/setup
```

- 3 次のコマンドを実行します。

```
./uninstall-sentinel
```

スクリプトによって、コレクタマネージャまたは関連エンジンとすべての関連データが完全に削除されるという警告が表示されます。

- 4 「y」と入力して、コレクタマネージャまたは関連エンジンを削除します。

スクリプトはまずサービスを停止し、その後に削除を実行します。ただし、コレクタマネージャと関連エンジンのアイコンは、Web インタフェースにインアクティブな状態で表示されたままです。

- 5 次の追加の手順を行って、Web インタフェースのコレクタマネージャと関連エンジンを手動で削除します：

コレクタマネージャ：

1. [イベントソースの管理] > [ライブビュー] にアクセスします。
2. 削除するコレクタマネージャを右クリックして、[削除] をクリックします。

関連エンジン：

1. 管理者として Sentinel Web インタフェースにログインします。
2. [相関関係] を展開してから、削除する関連エンジンを選択します。
3. [削除] ボタン (ごみ箱アイコン) をクリックします。

B.2.3 NetFlow コレクタマネージャのアンインストール

NetFlow コレクタマネージャをアンインストールするには、以下の手順に従います。

- 1 NetFlow コレクタマネージャのコンピュータにログインします。

注： NetFlow コレクタマネージャのインストールに使用したのと同じユーザ許可でログインする必要があります。

- 2 以下のディレクトリに変更します。

```
/opt/novell/sentinel/setup
```

3 次のコマンドを実行します。

```
./uninstall-sentinel
```

4 [y] を入力して、コレクタマネージャをアンインストールします。

スクリプトはまずサービスを停止してから、完全にアンインストールします。

B.3 アンインストール後の作業

Sentinel サーバをアンインストールしても、Sentinel 管理者ユーザはオペレーティングシステムから削除されません。このユーザを手動で削除する必要があります。

Sentinel のアンインストール後も、特定のシステム設定が残ります。これらの設定は、Sentinel のクリーンインストールを実行する前に削除する必要があります。特に、Sentinel のアンインストール時にエラーが発生した場合にその必要があります。

Sentinel のシステム設定を手動でクリーンアップするには：

1 root としてログインします。

2 すべての Sentinel プロセスを停止します。

3 /opt/novell/sentinel または Sentinel ソフトウェアがインストールされていた場所の内容を削除します。

4 Sentinel 管理者オペレーティングシステムユーザ (デフォルトでは novell) としてログインしているユーザがないことを確認してから、ユーザ、ホームディレクトリ、およびグループを削除します。

```
userdel -r novell
```

```
groupdel novell
```

5 オペレーティングシステムを再起動します。

